ON CERTAIN NUMERICAL INVARIANTS OF ALGEBRAIC VARIETIES WITH APPLICATION TO ABELIAN VARIETIES

BY

SOLOMON LEFSCHETZ

(Continued from p. 406)

§ 3. The characteristic equation is irreducible and Abelian

90. The first problem which presents itself is that of the determination of the indices. This determination will result from the following theorem:

In order that the matrix

$$\Omega \equiv \| 1, \alpha_j, \alpha_j^2, \cdots, \alpha_j^{2p-1} \| \qquad (j = 1, 2, \cdots, p),$$

where the (α)'s are roots of an irreducible Abelian equation $F(\alpha) = 0$ with $\bar{\alpha}_j = \alpha_{p+j}$, be impure, it is necessary and sufficient that the group G of the equation contain a subgroup G' maintaining the set $\alpha_1, \alpha_2, \cdots, \alpha_p$ invariant.

In order that Ω be impure it is necessary and sufficient that there exist a pair of non-conjugate roots (α_m, α_n) which cannot be deduced from a pair of roots with indices $\leqq p$ by any substitution of G. We shall have $\alpha_n = U\alpha_m$, where U is a well-defined substitution of G. If α_j is a root of index $< p$, there will exist a substitution T such that $\alpha_m = T\alpha_j$. The root $T^{-1}\alpha_n$ must not be one of the roots $\alpha_1, \alpha_2, \cdots, \alpha_p$, hence it is the conjugate $S\alpha_k$ of a root α_k of index $k < p$, that is

$$S\alpha_k = T^{-1}\alpha_n = T^{-1}U\alpha_m = T^{-1}UT\alpha_j = U\alpha_j,$$

and hence $\alpha_k = S^{-1}U\alpha_j = SU\alpha_j$. This shows that the set $\alpha_1, \alpha_2, \cdots, \alpha_p$ is transformed into itself by SU which is not the substitution unity, if $U \neq S$, as is actually the case since $\alpha_m \neq \bar{\alpha}_n$. The condition is therefore necessary.

On the other hand, if a substitution T (which cannot be S) maintains invariant the set $\alpha_1, \alpha_2, \cdots, \alpha_p$, I say that the pair of roots (α_j, α_k) $(j, k \leqq p)$ cannot be permuted with a pair $(\alpha_h, ST\alpha_h)$. To begin with, this is equivalent to affirming that it cannot be permuted with $(\alpha_j, ST\alpha_j)$. For if $\alpha_j = T'\alpha_h$, the pair $(\alpha_h, ST\alpha_h)$ can be permuted with $(\alpha_j, T'ST\alpha_h)$ or $(\alpha_j, ST\alpha_j)$. Assume then that there exists a substitution U of G permuting (α_j, α_k) with this last pair. Since G is Abelian it possesses no other substitution than the identity maintaining a root invariant. Now U is certainly not the identity for then we would have $\alpha_k = ST\alpha_j$, which is im-

possible for ST permutes the set $\alpha_1, \alpha_2, \cdots, \alpha_p$ with $\alpha_{p+1}, \alpha_{p+2}, \cdots, \alpha_{2p}$, and hence $k > p$ contrary to our assumptions. We must therefore have $ST\alpha_j = U\alpha_j$, $\alpha_j = U\alpha_k$, and consequently $U = ST$, $\alpha_j = ST\alpha_k$, which leads to a similar contradiction: $j > p$. It follows that G may not contain any substitution such as U. There is then a pair of conjugate roots which may not be derived from those of indices $\leqq p$ by substitutions of G, and Ω is impure, as was to be proved.

91. Let n be the order of G', assumed now to be the maximum subgroup maintaining invariant the set of multipliers $\alpha_1, \alpha_2, \cdots, \alpha_p$. G' does not contain S, hence the product of G' by S is a subgroup of order $2n$ of G. It follows that $2n$ divides the order $2p$ of G, and therefore n divides p. The roots $\alpha_1, \alpha_2, \cdots, \alpha_{2p}$ can be subdivided into $2p'$ sets of n roots, each set being composed of the roots derived from one of them by the substitutions of G'. Of these sets, p', say $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, $(\alpha_{n+1}, \cdots, \alpha_{2n})$, $\cdots$, $(\alpha_{(p'-1)n+1}, \cdots, \alpha_{p'n})$, form the set of p multipliers.

Let us designate by $A_1, A_2, \cdots, A_{p'}$ these sets of roots, and by $A_{p'+j}$ the set formed by the conjugate roots of those which compose A_j. Any substitution of G which does not belong to G' merely permutes the (A)'s among themselves. Moreover there exists none maintaining invariant the set $(A_1, A_2, \cdots, A_{p'})$ for otherwise G' would not be the maximum subgroup maintaining invariant the set of multipliers $(\alpha_1, \alpha_2, \cdots, \alpha_p)$. The group $G'' = G/G'$ of permutations of the (A)'s is also Abelian and we can apply to G'' and the (A)'s the same reasoning as before to G and the (α)'s. In particular the pai s $(A_j, A_{p'+j})$ are the only pairs which may not be derived from the pairs (A_j, A_k) of indices $j, k \leqq p'$, by the substitutions of G''. Let then α_j, α_k be a pair of roots and $A_{j'}, A_{k'}$ the (A)'s to which they belong. If the difference $j' - k' \neq \pm p'$, there exists a substitution of G'' permuting the pair $(A_{j'}, A_{k'})$ with a pair $(A_{j''}, A_{k''})$ of indices $j'', k'' \leqq p'$. This substitution permutes (α_j, α_k) with a pair of roots of indices $\leqq p$ and (α_j, α_k) is not an excluded pair. Moreover, in order that (α_j, α_k) be not excluded, it is necessary that $(A_{j'}, A_{k'})$ be permutable with a pair $(A_{j''}, A_{k''})$, $(j'', k'' \leqq p')$, which requires that $j' - k' \neq \pm p'$. Hence, the only pairs excluded are those for which $j' - k' = \pm p'$ and these pairs are all effectively excluded. Their number is $p + t = n^2 p' = np$, and therefore finally

$$1 + h = 2(1 + k) = 2np.$$

Remark: Let there be a set of roots $\alpha_1, \alpha_2, \cdots, \alpha_{p+qn}$, composed of $p' + q$ groups A_i, say $A_1, A_2, \cdots, A_{p'+q}$. Then from the pairs of roots (α_j, α_k) of indices $j, k \leqq p + qn$, we may certainly derive all pairs of roots without exception. This is an immediate consequence of the fact that among the (A)'s of the above set there are at least two whose indices differ by p'.

92. We shall now endeavor to obtain the structure of Ω when it is impure. For this purpose let

$$\beta_{q,\,s} = \alpha^s_{(q-1)n+1} + \alpha^s_{(q-1)n+2} + \cdots + \alpha^s_{qn}$$

and observe that Ω is isomorphic to a matrix Ω' whose p' first rows are

$$\begin{array}{llll} \beta_{1,\,1}, & \beta_{1,\,2}, & \cdots, & \beta_{1,\,2p} \\ \beta_{2,\,1}, & \beta_{2,\,2}, & \cdots, & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ \beta_{p',\,1}, & \cdots, & \cdots, & \beta_{p',\,2p}. \end{array}$$

The (β)'s are invariant under the substitutions of G' and those belonging to the same index s are permuted among themselves by the substitutions of G''. Consider, then, the equations in the unknowns n_i

$$n_1\,\beta_{s,\,1} + n_2\,\beta_{s,\,2} + \cdots + n_{2p}\,\beta_{s,\,2p} = 0 \qquad (s = 1, 2, \cdots, 2p').$$

The array of the coefficients is composed of $2p'$ rows derived from the determinant which may be formed with the periods of Ω' and their conjugates, hence the array is of rank $2p'$ and these equations are independent. Since G merely permutes them among themselves, they possess $2(p - p')$ independent rational solutions, and Ω' and hence Ω is isomorphic to a matrix

$$\left\| \begin{array}{ll} \omega, & 0 \\ 0, & \Omega_1 \end{array} \right\|;$$

$$\omega \equiv \|\, \beta_{j,\,h_1}, \beta_{j,\,h_2}, \cdots, \beta_{j,\,h_{2p'}} \,\| \qquad (j = 1, 2, \cdots, p'),$$

the indices $h_1, h_2, \cdots, h_{2p'}$ being chosen so that there exists no relation

$$d_1\,\beta_{j,\,h_1} + d_2\,\beta_{j,\,h_2} + \cdots + d_{2p'}\,\beta_{j,\,h_{2p'}} = 0$$

with integer coefficients d_i. For every other $\beta_{j,\,s}$ there will exist a relation

$$\beta_{j,\,s} = e_1\,\beta_{j,\,h_1} + e_2\,\beta_{j,\,h_2} + \cdots + e_{2p'}\,\beta_{j,\,h_{2p'}} \qquad (j = 1, 2, \cdots, 2p'),$$

where the (e)'s are rational. Hence an arbitrary rational function of the (α)'s belonging to the group G'' is of the form

$$\beta_1 = c_1\,\beta_{1,\,h_1} + c_2\,\beta_{2,\,h_1} + \cdots + c_{2p'}\,\beta_{2p',\,h_1},$$

where the (c)'s are rational numbers and the $2p' - 1$ conjugate values $\beta_2, \beta_3, \cdots, \beta_{2p'}$ of the algebraic domain determined by the multipliers are given by

$$\beta_j = c_1\,\beta_{j,\,h_1} + c_2\,\beta_{j,\,h_2} + \cdots + c_{2p'}\,\beta_{j,\,h_{2p'}}.$$

We then have $\beta_{j,\,h_s} = g_s(\beta_j)$, where the (g)'s are polynomials of degree $2p' - 1$ at most with rational coefficients and ω is therefore isomorphic to

$$\|\, g_1(\beta_j), g_2(\beta_j), \cdots, g_{2p'}(\beta_j) \,\| \qquad (j = 1, 2, \cdots, p'),$$

and finally to

$$\| 1, \beta_j, \beta_j^2, \cdots, \beta_j^{2p'-1} \| \qquad (j = 1, 2, \cdots, p').$$

Now $\beta_1, \beta_2, \cdots, \beta_{2p'}$ are roots of an irreducible Abelian equation of order $2p'$ whose group is G'' and no subgroup of G'' maintains the set $(\beta_1, \beta_2, \cdots, \beta_{p'})$ invariant, this always because G' is the maximum subgroup of G maintaining invariant the set $(\alpha_1, \alpha_2, \cdots, \alpha_p)$. Hence ω is pure and its indices h', k' are given by $1 + h' = 2(1 + k') = 2p'$. As to Ω, it is isomorphic to a matrix

$$\left\| \begin{matrix} \omega, & 0, & \cdots, & 0 \\ 0, & \omega, & \cdots, & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots, & \omega \end{matrix} \right\|$$

with n terms in the principal diagonal, as results from the fact that the reduction to the type (II) is unique. For its invariants we have then

$$1 + h = n^2(1 + h') = 2n^2 p';$$

hence

$$1 + h = 2(1 + k) = 2n^2 p' = 2np,$$

as we have already shown in a different manner in No. 91.

93. The multiplications of Ω can be found without difficulty and in fact in two different ways. For let $\alpha_{in+1}, \alpha_{in+2}, \cdots, \alpha_{(i+1)n}$ be again a set of multipliers permuted by the subgroup G' of order n. The system of numbers λ_{jk} given by the array

$$\left\| \begin{matrix} E_1, & 0, & \cdots, & 0 \\ 0, & E_2, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots, & E_{p'} \end{matrix} \right\|,$$

$$E_{i+1} \equiv \left\| \begin{matrix} g_1(\alpha_{in+1}), & g_2(\alpha_{in+1}), & \cdots, & g_n(\alpha_{in+1}) \\ g_n(\alpha_{in+2}), & g_1(\alpha_{in+2}), & \cdots, & g_{n-1}(\alpha_{in+2}) \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ g_2(\alpha_{(i+1)n}), & g_3(\alpha_{(i+1)n}), & \cdots, & g_1(\alpha_{(i+1)n}) \end{matrix} \right\|,$$

where the (g)'s are arbitrary polynomials of degree $2p - 1$ with rational coefficients, defines a complex multiplication, and as we have here a linear system with $2np = 1 + h$ parameters, every multiplication is of this type.

We may also obtain the multiplications in a different manner. The multiplications of the matrix Ω' to which Ω was reduced in No. 92, which depends upon those obtained by transforming the submatrix ω into itself or into another like it, are of the general type $\| E_{\mu\nu} \|$ $(\mu, \nu = 1, 2, \cdots, n)$, where the (E)'s are

matrices representing multiplications of ω, that is of the type

$$E_{\mu\nu} \equiv \left\| \begin{array}{cccc} g_{\mu\nu}(\beta_1), & 0, & \cdots, & 0 \\ 0, & g_{\mu\nu}(\beta_2), & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots, & g_{\mu\nu}(\beta_{p'}) \end{array} \right\|,$$

where the (g)'s are arbitrary polynomials of degree $2p' - 1$ with rational coefficients. As we have here again $2n^2 p' = 1 + h$ distinct multiplications of Ω', all its multiplications are of this type.—On the other hand if Λ, Λ' are corresponding multiplications of Ω, Ω', we have $\Lambda' = M\Lambda M^{-1}$, where M is a definite square matrix of order p. Hence having obtained all the multiplications of one of them, we may say that we also possess all those of the other.

It is of interest to consider the multipliers η_i of Λ, which are the same as those of Λ'. The latter being assumed as the multiplication written above, on forming the equation in the (η)'s, we see at once that it is obtained by multiplying the left-hand sides of the p' equations of degree n

$$\phi(\eta;\ \beta_i) = |g_{\mu\nu}(\beta_i) - \epsilon_{\mu\nu}\,\eta| = 0$$
$$(i = 1, 2, \cdots, p'; \quad \mu, \nu = 1, 2, \cdots, n; \quad \epsilon_{\mu\nu} = 1; \quad \epsilon_{\mu\nu} = 0, \mu \neq \nu),$$

where ϕ is a polynomial in η and β_i with rational coefficients, and moreover the conjugates $\eta_{p+1}, \eta_{p+2}, \cdots, \eta_{2p}$ of the (η)'s satisfy the equations $\phi(\eta;\ \beta_{p'+i}) = 0$. Two cases may now present themselves: (*a*) These $2p'$ equations have all the same roots. Then $\phi(\eta;\ \beta_i) = 0$ reduces to an equation $\phi(\eta) = 0$ in η alone, of degree at most n. We can take for ϕ an arbitrary polynomial with rational coefficients since Ω' is equivalent to a matrix composed with arrays

$$\tau \equiv \| \tau_{j1}, \tau_{j2}, \cdots, \tau_{j,2p'} \|, \quad \| 1, \eta_j, \eta_j^2, \cdots, \eta_j^{n-1} \| \qquad (j = 1, 2, \cdots, p),$$

where η_j is an arbitrary root of $\phi(\eta) = 0$, and the array τ is composed of the matrix ω superposed n times. Generally speaking we shall obtain all the multiplications of the nature here considered if we succeed in forming all the polynomials with rational coefficients $g_{\mu\nu}(\beta_i)$ such that the coefficients of the polynomial $\phi(\eta;\ \beta_i)$ in η are independent of β_i, that is, are rational numbers. (*b*) Among the $2p'$ equations in the multipliers η_i there are at least two whose roots are not the same. In this case the adjunction of one of the (β)'s to the domain of rationality brings about the reduction of the equation in the multipliers if that equation is not reducible already. In particular, if the new multiplication does not transform into themselves certain submatrices and if it is of degree $> n$, the equation in the multipliers is necessarily reducible in the domain of rationality $K(\beta_i)$, hence in the domain $K(\alpha_i)$.

94. To complete this investigation it is necessary to compare from the point

of view of isomorphism two matrices

$$\Omega \equiv \| 1, \alpha_{j_n}, \alpha_{j_n}^2, \cdots, \alpha_{j_n}^{2p-1} \| ; \quad \Omega' \equiv \| 1, \alpha_{h_n}, \alpha_{h_n}^2, \cdots, \alpha_{h_n}^{2p-1} \|$$

$(n = 1, 2, \cdots, p)$, corresponding to the same equation $F(\alpha) = 0$.

In order that Ω, Ω' be isomorphic there must exist a simultaneous bilinear form

$$\sum c_{\mu\nu}\, x_\mu\, y_\nu .$$

By reasoning as at the beginning of § 2, we see that we must have

$$\sum_{\mu,\nu} c_{\mu\nu} (\alpha_j^{\mu-1} \alpha_h^{\nu-1} - \alpha_j^{\nu-1} \alpha_h^{\mu-1}) = 0$$

whenever (α_j, α_h) is a pair of roots derived from the pairs $(\alpha_{j_m}, \alpha_{h_n})$ $(m, n = 1, 2, \cdots, p)$, by the substitutions of the group G. If the pairs thus derived include all pairs of roots, the system of equations will have as many independent equations as there are unknowns $c_{\mu\nu}$, and these unknowns will all be zero so that Ω, Ω' will not be isomorphic.

Thus as a condition for isomorphism, we find that it must not be possible to derive from the pairs $(\alpha_{j_m}, \alpha_{h_n})$ all the possible pairs of roots. Let (α_q, α_r) be an excluded pair and U, T substitutions of G such that $\alpha_r = U\alpha_q$, $\alpha_{j_m} = T\alpha_q$. It must not be possible for T to permute α_r with an α_{h_n}, hence T must permute it with an α_{h_n}, and therefore $T\alpha_r = S\alpha_{h_n}$. It follows that $TU\alpha_q = S\alpha_{h_n} = U\alpha_{j_m}$, which shows that SU permutes the set $(\alpha_{j_1}, \alpha_{j_2}, \cdots, \alpha_{j_p})$ with the set $(\alpha_{h_1}, \alpha_{h_2}, \cdots, \alpha_{h_p})$. Thus in order that Ω and Ω' be isomorphic, it is necessary that there exist a subgroup of G permuting these two sets.

Conversely let T be a substitution permuting these two sets. No pair $(\alpha_{j_1}, \alpha_{h_1})$ may be permuted with $(\alpha_m, ST\alpha_m)$. For let U be the substitution of G such that $U\alpha_{j_1} = \alpha_m$. We must have $U\alpha_{h_1} = ST\alpha_m$, hence $\alpha_{h_1} = ST\alpha_{j_1}$, from which would follow that α_{h_1} belongs to both sets $(\alpha_{h_1}, \alpha_{h_2}, \cdots, \alpha_{h_p})$, $(\bar{\alpha}_{h_1}, \alpha_{h_2}, \cdots, \bar{\alpha}_{h_p})$—an impossibility. Hence Ω, Ω' certainly possess a simultaneous form. If they are pure this is sufficient to insure their isomorphism. Assume that they are impure, and let ω, ω' be the corresponding pure matrices after the manner of No. 92, β_j, β'_j the quantities analogous to those already designated by similar letters corresponding to these two matrices. It is seen at once that since the sets $(\alpha_{j_1}, \alpha_{j_2}, \cdots, \alpha_{j_p})$, $(\alpha_{h_1}, \alpha_{h_2}, \cdots, \alpha_{h_p})$ are permuted by some substitution of G, the subgroups which maintain them invariant coincide. Hence ω, ω' are of the same genus p', and the (β)'s and (β')'s can be taken as roots of one and the same irreducible equation of degree $2p'$. Moreover to

$$\beta_j = \alpha_{n(j-1)} + \alpha_{n(j-1)+1} + \cdots + \alpha_{nj}$$

corresponds

$$\beta'_j = T\alpha_{n(j-1)} + T\alpha_{n(j-1)+1} + \cdots + T\alpha_{nj} .$$

Hence the sets $(\beta_1, \beta_2, \cdots, \beta_{p'})$, $(\beta'_1, \beta'_2, \cdots, \beta'_{p'})$ are permuted by a substitution of the group of the equation in the (β)'s and therefore ω, ω' are isomorphic, from which follows that this is also the case for Ω, Ω'. Thus *in order that* Ω, Ω' *be isomorphic, it is necessary and sufficient that there exist a substitution of the group* G *permuting their sets of multipliers.*

Corollary. The number of essentially distinct matrices belonging to $F(\alpha)$ *is equal to its number of classes of transitively permutable sets of* p *roots.*

This ends the discussion of the case where $F(\alpha)$ is irreducible, Abelian.

§ 4. Characteristic equation of type $[f(\alpha)]^r = 0$, $r > 1$. (*a*) Generalities

95. We assume of course $f(\alpha)$ irreducible and shall denote its degree as previously by q. The matrix Ω is composed with two arrays

$$\tau \equiv \| \tau_{j1}, \tau_{j2}, \cdots, \tau_{jr} \|, \quad \| 1, \alpha_j, \alpha_j^2, \cdots, \alpha_j^{q-1} \| \qquad (j = 1, 2, \cdots, p;\ qr = 2p),$$

where the (α)'s are roots of $f(\alpha) = 0$. We recall that if α_j is real it must be double root of $f = 0$, hence r must be even.

In order that Ω be a Riemann matrix it is necessary that there exist rational numbers $c_{\mu\nu}^{mn}$, such that

$$\sum_{m,n}^{1\ldots q} \sum_{\mu,\nu}^{1\ldots r} c_{\mu\nu}^{mn} (\alpha_j^{m-1} \alpha_h^{n-1} \tau_{j\mu} \tau_{h\nu} - \alpha_j^{n-1} \alpha_h^{m-1} \tau_{j\nu} \tau_{h\mu}) = 0 \qquad (j, h = 1, 2, \cdots, p). \tag{11}$$

Let us set

$$\gamma_{\mu\nu}(\alpha_j, \alpha_h) = \sum_{m,n} c_{\mu\nu}^{mn} \alpha_j^{m-1} \alpha_h^{n-1} \qquad (\gamma_{\mu\nu}(x, y) = -\gamma_{\nu\mu}(y, x)).$$

We may say that the array τ will possess the bilinear forms

$$\sum_{\mu,\nu} \gamma_{\mu\nu}(\alpha_j, \alpha_h) x_\mu y_\nu \qquad (j, h = 1, 2, \cdots, p), \tag{12}$$

in the sense that the particular form corresponding to (α_j, α_h) must vanish when we replace in it the (x)'s by the elements of the j-th row and the (y)'s by those of the h-th column. We shall say for the sake of simplicity that this form (12) is a bilinear form of Ω.

In order that Ω be a Riemann matrix, it is necessary besides that

$$\sum_{j,h}^{1\ldots p} A_{jh} x_j \bar{x}_h; \quad A_{jh} = \frac{-1}{2i} \sum \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_h) \tau_{j\mu} \bar{\tau}_{h\nu} \tag{13}$$

be a positive definite Hermitian form. We shall assume this condition fulfilled for the present and will return to it later. The relations thus imposed upon the elements of τ do not determine them completely and they will depend in general upon a certain number of essential parameters. We have

thus classes of Riemann matrices and our object will be to determine the invariants of the most general matrix of a given class.

96. Assume then that there exists a single form (12). What are the invariants of Ω? The numbers $c_{\mu\nu}^{mn}$ corresponding to a given Riemann form must always satisfy the relations (11) and as the $\gamma_{\mu\nu}(\alpha_j, \alpha_h)$ are uniquely determined up to a factor of proportionality necessarily rational in α_j, α_h, we have

$$\sum_{m,n}^{1\ldots q} c_{\mu\nu}^{mn}\, \alpha_j^{m-1}\, \alpha_h^{n-1} = \phi_{jh}(\alpha_j, \alpha_h)\, \gamma_{\mu\nu}(\alpha_j, \alpha_h) \qquad (j \neq h;\ j, h = 1, 2, \cdots, p),$$

where ϕ_{jh} is a polynomial with rational coefficients. The left-hand side must be changed in sign when we interchange at the same time j, h and μ, ν. Hence

$$\phi_{jh}(\alpha_j, \alpha_h) = \phi_{jh}(\alpha_h, \alpha_j) = \phi_{hj}(\alpha_h, \alpha_j),$$

that is, ϕ_{jh} must be symmetrical in α_j and α_h. Moreover if the group G of $f(\alpha) = 0$ permutes the pairs (α_j, α_h) and $(\alpha_{j'}, \alpha_{h'})$, then it is necessary that $\phi_{jh}(x, y) = \phi_{j'h'}(x, y)$. Finally if there are equal roots among the multipliers $\alpha_1, \alpha_2, \cdots, \alpha_p$, say $\alpha_j = \alpha_{j'}$—which is certainly the case if $r > 2$—and if moreover the quantities $\gamma_{\mu\nu}(\alpha_j, \alpha_j)$ are not all zero, we will have to consider a unique function $\phi^j(\alpha_j) = \phi_{jj'}(\alpha_j, \alpha_{j'})$. This will certainly occur when the (α)'s are all real, for then in order that (13) be definite none of the quantities A_{jj} must be zero, hence the expressions $\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) = \gamma_{\mu\nu}(\alpha_j, \alpha_j)$ must not all be zero either.

Given the (γ)'s and the (ϕ)'s, the numbers $c_{\mu\nu}^{mn}$, when μ, ν are assigned, satisfy a system of non-homogeneous linear equations whose number is determined thus:

(*a*) Among the multipliers $\alpha_1, \alpha_2, \cdots, \alpha_p$ two at least are equal. Let then s be the number of pairs of distinct roots derived from the pairs α_j, α_h; $j, h < p$, by the substitutions of G. When $\mu \neq \nu$ there are $2s + q$ equations and when $\mu = \nu$ there are s of them.

(*b*) The multipliers $\alpha_1, \alpha_2, \cdots, \alpha_p$ form without repetition the totality of the roots of $f(\alpha) = 0$. This occurs only when $p = q$, $r = 2$. The number of equations is then $q(q-1)$ or $\frac{1}{2}q(q-1)$ according as $\mu \neq \nu$ or $\mu = \nu$.

But as we have seen in § 2, the left-hand sides of the equations in the $(c_{\mu\nu})$'s, when these unknowns are considered as variables, are linearly independent. Hence when the (γ)'s and the (ϕ)'s are given we have a solution with

$$r\left[\binom{q}{2} - s\right] + 2\binom{r}{2}\left[\binom{q}{2} - s\right] = r^2\left[\binom{q}{2} - s\right]$$

arbitrary parameters in the first case and with $q = p$ of them in the second.

It remains to determine the number of systems

$$\phi^1_{jh},\ \phi^2_{jh},\ \cdots,\ \phi^n_{jh};\ \phi^1(\alpha_j),\ \phi^2(\alpha_j),\ \cdots,\ \phi^n(\alpha_j)$$

such that there exist no relations

$$\sum_{t=1}^{n} \lambda_t\, \phi^t_{jh}(\alpha_j,\ \alpha_h) = 0, \quad \sum_{t=1}^{n} \lambda_t\, \phi^t(\alpha_j) = 0,$$

where the (λ)'s are rational numbers and where we must replace in the second relation α_j successively by all the roots of $f(\alpha) = 0$, and in the first $(\alpha_j,\ \alpha_h)$ by all the pairs of distinct roots, derived from those for which $j,\ h \leqq p$, by the substitutions of G. Moreover, in case (*b*) or in case (*a*) when the $\gamma_{\mu\nu}(\alpha_j,\ \alpha_j)$ are all zero we must make $\phi(\alpha_j) \equiv 0$. Between the symmetrical functions $\alpha_j^m\, \alpha_h^n + \alpha_j^n\, \alpha_h^m$ of two assigned roots there must exist a certain number t_i of linear homogeneous relations with integral coefficients, and these relations will still be satisfied by the symmetrical functions of two roots $T\alpha_j,\ T\alpha_h$, where T is an arbitrary substitution of G. The number t_i of linearly independent symmetrical functions characterizes therefore not so much the pair $(\alpha_j,\ \alpha_h)$ as the set of pairs of roots which are transitively permutable with it by the substitutions of G,—and to each set of transitively permutable pairs of roots corresponds such an integer. Let finally ϵ be a number $= 0$ if $\phi(\alpha_j) \equiv 0$ and $= +1$ if $\phi(\alpha_j) \not\equiv 0$. A very simple discussion shows then that in case (*a*)

$$1 + k = \epsilon q + \sum t_i + r^2 \left[\binom{q}{2} - s \right],$$

while in case (*b*)

$$1 + k = \sum t_i + p.$$

The determination of h can be made in a similar manner. If we assume the array τ as general as possible, there will be no other relations between its elements than those which follow from the existence of (11). A non-alternate bilinear form must then correspond to the relations

$$\sum_{m,n}^{1\ldots q} \sum_{\mu,\nu}^{1\ldots r} c^{mn}_{\mu\nu}\, \alpha_j^{m-1}\, \alpha_h^{n-1}\, \tau_{j\mu}\, \tau_{h\nu} = 0 \qquad (j,\ h = 1,\ 2,\ \cdots,\ p),$$

whence we will derive as before

$$\sum_{m,n} c^{mn}_{\mu\nu}\, \alpha_j^{m-1}\, \alpha_h^{n-1} = \phi_{jh}(\alpha_j,\ \alpha_h)\, \gamma_{\mu\nu}(\alpha_j,\ \alpha_h), \tag{14}$$

where ϕ_{jh} is no more constrained to be symmetrical. We shall now have to consider as distinct the pairs of roots $(\alpha_j,\ \alpha_h)$ and $(\alpha_h,\ \alpha_j)$, and in place of t_i we shall be led to introduce an integer t'_i to denote the number of products $\alpha_j^m\, \alpha_h^n$ between which there exists no linear relation with integral coefficients.

Finally, we have

$$1 + h = \epsilon q + \sum t_i' + 2r^2\left[\binom{q}{2} - s\right]$$

in case (a), ϵ having the same meaning as previously, while in case (b)

$$1 + h = \sum t_i' + p.$$

If there exists a non-identically zero solution of the equations (11) and (14) and the (γ)'s are not all zero, it will be necessary to add to k and h respectively the numbers

$$r^2\left[\binom{q}{2} - s\right], \qquad 2r^2\left[\binom{q}{2} - s\right]$$

in case (a), and the same number p in case (b).

Remark: It is not difficult to extend these formulas to the case where Ω possesses several bilinear forms of the type considered. However, the results obtained are not simple and it is preferable to establish them directly in the few cases where this extension will be needed.

97. As an application of the preceding considerations, consider the case where $f(\alpha) = 0$ is as general as possible and of degree $q > 2$. The group G is then the symmetrical group, hence doubly transitive. There will then be a single integer $t_i = t$ and a single integer $t_i' = t'$. To find t' observe that the equations in the unknowns d_{mn},

$$\sum_{m,n}^{1\cdots q} d_{mn}\, \alpha_j^{m-1} \alpha_h^{n-1} = 0 \qquad (j, h = 1, 2, \cdots, q; j \neq h), \tag{15}$$

possess q independent rational solutions. Hence there are

$$q^2 - q = q(q-1) = t'$$

products $\alpha_j^m \alpha_h^n$ between which there exist no linear relations with integral coefficients, and therefore $1 + h = q(q-1) + \epsilon q$. The number of distinct symmetrical functions formed with the products

$$\alpha_j^m \alpha_h^n \qquad (m, n < q) \qquad \text{is equal to} \qquad \tfrac{1}{2}q(q-1) + q = \tfrac{1}{2}q(q+1).$$

But between them there are as many linear relations with integral coefficients as there are independent solutions of the equations in the unknowns d_{mn},

$$\sum_{m,n}^{1\cdots q} d_{mn}\left(\alpha_j^{m-1} \alpha_h^{n-1} + \alpha_j^{n-1} \alpha_h^{m-1}\right) = 0 \qquad (j, h = 1, 2, \cdots, q; j \neq h).$$

But these equations are linear combinations of the equations (15), and the manner in which they have been obtained shows that they are independent like the equations (15) themselves. They possess therefore

$\frac{1}{2}q(q+1) - \frac{1}{2}q(q-1) = q$ independent solutions and hence

$$1 + k = t = \frac{q(q+1)}{2} - q = \frac{q(q-1)}{2}.$$

98. We shall now examine more closely the *conditions of existence of* Ω. Let us return to the form (12). We may define two polynomials with integral coefficients

$$\gamma'_{\mu\nu}(x, y) = \sum_{m,n}^{1\cdots q} d^{mn}_{\mu\nu} x^{m-1} y^{n-1},$$
$$\gamma''_{\mu\nu}(x) = \sum_{m=1}^{q} d^{m}_{\mu\nu} x^{m-1}$$

by the relations

$$\gamma'_{\mu\nu}(\alpha_j, \alpha_k) = \gamma_{\mu\nu}(\alpha_j, \alpha_h) \qquad (\alpha_j, \alpha_k \text{ are any two different roots});$$
$$\gamma'_{\mu\nu}(\alpha_j, \alpha_j) = 0; \qquad \gamma''_{\mu\nu}(\alpha_j) = \gamma_{\mu\nu}(\alpha_j, \alpha_j) \qquad (j = 1, 2, \cdots, 2p).$$

Consider the elements of a given row of τ as homogeneous point coördinates in an S_{r-1}—this is the generalization of Scorza's habitual point of view. To the r_j rows corresponding to α_j (r_j is the number of times that α_j is found among the multipliers), say

$$\begin{matrix} \tau'_{11}, & \tau'_{12}, & \cdots, & \tau'_{1r} \\ \tau'_{21}, & \cdot & \cdots, & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \tau'_{r_j1}, & \cdot & \cdots, & \tau'_{r_jr} \end{matrix}$$

will correspond an S_{r_j-1}. The equations (11) can be interpreted as follows:

(*a*) S_{r_j-1} and S_{r_k-1} must be conjugate spaces relatively to the reciprocity

$$\sum_{\mu,\nu}^{1\cdots r} \gamma'_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu = 0.$$

(*b*) Any two points of S_{r_j-1} are conjugate relatively to the linear complex

$$\sum_{\mu,\nu}^{1\cdots r} \gamma''_{\mu\nu}(\alpha_j) x_\mu y_\nu = 0.$$

(*c*) In the Hermitian form (13) let us annul all variables corresponding to roots other than α_j. The remaining expression is, with a change in the indices of the (x)'s,

$$-\frac{1}{2i}\sum_{h,k}^{1\cdots r_j}\sum_{\mu,\nu}^{1\cdots r} \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j)\tau_{h\mu}\tau_{k\nu} x_h \bar{x}_k.$$

It must be positive for all non-zero values of the (x)'s. Now it may be written

$$-\frac{1}{2i}\sum_{\mu,\nu}^{1\cdots r} \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j)\sum_{h=1}^{r_j}\tau'_{h\mu} x_h \sum_{k=1}^{r_j}\bar{\tau}'_{k\nu}\bar{x}_k,$$

which shows that this amounts to requiring that the Hermitian form

$$-\frac{1}{2i}\sum_{\mu,\nu}^{1\cdots r}\gamma_{\mu\nu}(\alpha_j,\,\bar{\alpha}_j)\,x_\mu\,\bar{x}_\nu$$

be positive for all points of S_{r_j-1}.

99. The condition (c) may be interpreted in two distinct ways according as α_j is real or complex:

(c') If α_j is real it is equivalent to demanding that the real complex

$$\sum \gamma''_{\mu\nu}(\alpha_j)\,x_\mu\,y_\nu = 0$$

contain no real straight line resting on S_{r_j-1}.

(c'') If α_j is complex the Hermitian form

$$-\frac{1}{2i}\sum \gamma'_{\mu\nu}(\alpha_j,\,\bar{\alpha}_j)\,x_\mu y_\nu$$

must be positive at all points of S_{r_j-1}.

The conditions (a), (b), (c'), (c'') are necessary but may not be sufficient. Hence if there exist Riemann matrices for which these conditions but no others are fulfilled, these matrices will certainly be as general as possible of their type, and their invariants will be as small as possible.

Returning to (c''), denote for the present by $S_{r'_j-1}$ the space corresponding to α_j. The Hermitian form above may also be written

$$\frac{1}{2i}\sum \gamma'_{\mu\nu}(\alpha_j,\,\bar{\alpha}_j)\,x_\mu\,\bar{x}_\nu = -\frac{1}{2i}\sum \gamma'_{\mu\nu}(\alpha_j,\,\bar{\alpha}_j)\,\bar{x}_\mu\,x_\nu\,.$$

This shows that it must be positive at all points of S_{r_j-1} and negative at all those of $\bar{S}_{r'_j-1}$, conjugate space of $S_{r'_j-1}$.

Now it is known from classical theorems on Hermitian forms that by means of a transformation

$$x'_\mu = \sum_{\nu=1}^{r}\lambda_{\mu\nu}\,x_\nu;\qquad \bar{x}'_\mu = \sum_{\nu=1}^{r}\bar{\lambda}_{\mu\nu}\,\bar{x}_\nu \qquad (\mu = 1, 2, \cdots, r)$$

our form may be reduced to the type

$$\sum a_\mu\,x'_\mu\,\bar{x}'_\mu\,,$$

where the (a)'s are real. If we consider the transformation on the (x)'s as applied to the points of S_{r_j-1} and of $\bar{S}_{r'_j-1}$, and that on the $(\bar{x})$'s to the points of $S_{r'_j-1}$, we see that the mutual relations of the three spaces S, S', $\bar{S}'$, transformed of the three preceding, are again the same as before in regard to the new Hermitian form. Now however we have the advantage that the new form takes the same sign at S' and $\bar{S}'$, so that we have this situation: The spaces S and S' are conjugate with respect to the reciprocity obtained by making the

Hermitian form vanish, and the form takes the sign + on the one and the sign − on the other. We shall see later that this requires that $r = r_j + r'_j$. Hence the transformed form must not be degenerate and this holds also for the original one.

100. Let us make a few remarks concerning the equation $f(\alpha) = 0$ when it has mixed real and complex roots. We may show that in this case the integers r_j cannot in general be taken arbitrarily. For assume that the group G of the equation is doubly transitive, that is, permutes transitively all the pairs of roots. If one of the reciprocities

$$\sum \gamma'_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu = 0$$

is degenerate so will all the others be, since when the determinant

$$|\gamma'_{\mu\nu}(\alpha_j, \alpha_k)| \qquad (\mu, \nu = 1, 2, \cdots, r)$$

is zero for a pair of distinct roots, it will be zero for all of them. But as we have just seen this reciprocity is certainly not degenerate for $\alpha_j = \bar{\alpha}_k$, hence it is never degenerate when $\alpha_j \neq \alpha_k$.

Assume now α_j real, α_k still complex. S_{r_j-1} and S_{r_k-1} are conjugate relatively to the non-degenerate reciprocity

$$\sum \gamma'_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu = 0,$$

hence $r_j - 1 + r_k - 1 = r - 2$. But $r_j = \frac{1}{2}r$, hence $r_k = \frac{1}{2}r$ also. Thus all the (r)'s must have the value $\frac{1}{2}r$, that is, among the multipliers must be found every root of $f(\alpha) = 0$ taken the same number of times.

Let us return to the Hermitian form

$$-\frac{1}{2i}\sum \gamma'_{\mu\nu}(\alpha_j, \alpha_j) x_\mu \bar{x}_\nu.$$

It will have one sign on S_{r_j-1} and another on $\bar{S}_{r'_j-1}$. Hence, as we shall see below, the equation of degree r in δ,

$$|\gamma'_{\mu\nu}(\alpha_j, \alpha_j) - \epsilon_{\mu\nu}\cdot\delta| = 0 \qquad (\epsilon_{\mu\mu} = 1;\ \epsilon_{\mu\nu} = 0,\ \mu \neq \nu),$$

must have $\frac{1}{2}r$ positive roots and $\frac{1}{2}r$ negative roots. There is here considerable restriction imposed upon the form (12).

An interesting case of mixed equation has been investigated by Frobenius, —the case of the characteristic equation of a principal transformation. Frobenius does not give himself an arbitrary equation $f(\alpha) = 0$ but assumes a definite Riemann projectivity and starts from the equation

$$|b_{\mu\nu} - \epsilon_{\mu\nu}\cdot\alpha| = 0,$$

showing that, given such an equation, there always corresponds to it a suitable Riemann matrix.

101. Before continuing, let us examine rapidly the lower limits which may be assigned to h and k in some simple cases. First, if the multiplication has real multipliers, we will have necessarily $\epsilon = 1$, on account of (b) and (c'), hence $1 + h \geqq q$, $1 + k \geqq q$. Assume the multipliers all imaginary, hence $q = 2q'$. According to (a) and (c'') the expressions $\gamma_{\mu\nu}(\alpha_j, \alpha_j)$ must not all be zero. The group G of $f(\alpha) = 0$ may permute transitively a pair $(\alpha_j, \bar{\alpha}_j)$ with other pairs of roots.—Let $(\alpha_1', \alpha_1''), \cdots, (\alpha_{q''}', \alpha_{q''}'')$ be one of the sets thus transitively permuted and including a pair of conjugate roots. We have $\sum q'' \geqq q'$ and the (q'')'s are all > 1, if $q > 2$, else $f(\alpha)$ would be reducible. There can be no such relation as

$$\sum_{m,n}^{1\ldots q''} c_{mn}\, \alpha_j'^{\,m-1}\, \alpha_h''^{\,n-1} = 0 \qquad (j, h = 1, 2, \cdots, q''),$$

since the Vandermonde determinants of the (α')'s and (α'')'s are not zero. Similarly there can be no such relations as

$$\sum_{m,n}^{1\ldots q''} c_{mn}\,(\alpha_j'^{\,m-1}\, \alpha_h''^{\,n-1} + \alpha_j'^{\,n-1}\, \alpha_h''^{\,m-1}) = 0 \qquad (j, h = 1, 2, \cdots, q'').$$

Hence,

$$\sum t_i \geqq \sum \frac{q''(q''-1)}{2} \geqq \sum \frac{(q''-1)^2}{2} + \tfrac{1}{2} \sum q'',$$

and therefore if $q > 2$, $1 + k > \frac{1}{4}q$. Moreover since there are obviously q independent multiplications—namely q powers of the given one—we have $1 + h \geqq q$. These limits are obviously correct a fortiori if Ω is impure with submatrices invariant under the Riemann projectivity considered. In particular $k = 0$, $h > 0$ is possible only if $f(\alpha) = 0$ is a quadratic equation with imaginary roots. We shall return to this later.

§ 5. The characteristic equation is of type $[f(\alpha)]^r = 0$. (b) Two important special cases

102. *Real multipliers** $(r = 2p' > 2)$. When the multipliers are real, the integers r_j are all equal to p' and the only conditions to be satisfied are (b) and (c'). By a slight change in our notation we may say that it is first necessary that the points of S_{r_j-1} be conjugated to each other with respect to the linear complex

$$\sum_{\mu,\nu}^{1\ldots 2p'} \gamma_{\mu\nu}(\alpha_j)\, x_\mu\, y_\nu = 0. \tag{16}$$

Next at all points of S_{r_j-1} we must have

$$-\frac{1}{2i} \sum \gamma_{\mu\nu}(\alpha_j)\, x_\mu\, \bar{x}_\nu > 0.$$

* (Added in 1922.) See *Comptes Rendus du Congrès de Strasbourg* (1921).

Consider the matrix

$$\tau_j \equiv \| \tau^j_{h1}, \tau^j_{h2}, \cdots, \tau^j_{h,\,2p'} \| \qquad (j = 1, 2, \cdots, p'),$$

formed with the rows of τ which correspond to α_j. The last condition just stated is equivalent to requiring that the Hermitian forms

$$(17) \qquad \sum_{h,k}^{1\cdots p} A^j_{hk}\, x_h\, \bar{x}_k, \qquad A^j_{hk} = -\frac{1}{2i} \sum_{\mu,\nu}^{1\cdots 2p'} \gamma_{\mu\nu}(\alpha_j)\, \tau^j_{h\mu}\, \bar{\tau}^j_{k\nu}$$

be definite positive. Under these conditions I say that (16) defines a principal Riemann form of Ω. For we may determine a Riemann form

$$\sum \delta_{\mu\nu}(\alpha_j, \alpha_k)\, x_\mu\, y_\nu,$$

with coefficients $\delta_{\mu\nu}$ satisfying the relations

$$\begin{aligned} \delta_{\mu\nu}(\alpha_j, \alpha_k) &= 0 \qquad\qquad (\alpha_j \neq \alpha_k), \\ \delta_{\mu\nu}(\alpha_j, \alpha_j) &= \gamma_{\mu\nu}(\alpha_j), \end{aligned}$$

since the equations for the coefficients of the polynomials $\delta_{\mu\nu}$ always have at least one rational solution. On the other hand the Hermitian form corresponding to this Riemann form reduces to the sum of the forms (17),—it is therefore definite positive.

We may remark that in all cases if (16) corresponds to a non-principal-alternate form, the corresponding Hermitian form is the sum of the q forms (17), hence its genus is the sum of their genera.

Let us return to τ_j. It is clear that the conditions imposed upon this matrix are identical with the conditions imposed upon a Riemann matrix of genus p', except that the coefficients of the principal alternate form which occurs in the definition of these matrices are only subjected to being numbers of the algebraic domain $K(\alpha_j)$ but not necessarily rational numbers. We may say that τ_j is a Riemann matrix belonging to this algebraic domain.

103. By a transformation of coördinates with coefficients rational with respect to those of the complex (16), that is, with coefficients belonging to the domain $K(\alpha_j)$, we may reduce the equation of this complex to the form

$$\sum_{\mu=1}^{p'} e_\mu(\alpha_j)\,(x_\mu\, y_{p'+\mu} - x_{p'+\mu}\, y_\mu),$$

where the (e)'s are numbers of the same domain.* This is equivalent to applying a certain transformation of isomorphism upon Ω. By following up this transformation with q others applied each to the rows of τ_j, we shall reduce τ_j to the form

$$\left\| \begin{matrix} (e_1(\alpha_j))^{-1}, & 0, & \cdots, & 0, & a^j_{11}, & a^j_{12}, & \cdots, & a^j_{1p'} \\ 0, & (e_2(\alpha_j))^{-1}, & \cdots, & 0, & a^j_{21}, & a^j_{22}, & \cdots, & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots, & (e_{p'}(\alpha_j))^{-1}, & a^j_{p'1}, & \cdot & \cdots, & a^j_{p'p'} \end{matrix} \right\|$$

* See for example Bertini, *Lezzioni sulla geometria proiettiva degli iperspazi*, page 106.

and if we set $a^j_{hk} = a'_{hk} + ia''_{hk}$ it is necessary that the quadratic forms $\sum a''_{hk}\, x_h\, y_k$ be all definite positive.

The class of matrices thus obtained depends upon $\frac{1}{2}qp'(p'+1) = \frac{1}{4}p(r+2)$ continuous parameters, and $qp' = p$ arbitrary integers—the integers which enter into the composition of the (e)'s, where we may assume the coefficients of the powers of the (α)'s equal to integers.

The invariants of the most general matrices of the class here considered are given by

$$1 + h = 1 + k = q,$$

since with the notations of § 4, the (ϕ_{jh})'s are zero, $s = \binom{q}{2}$ and the expressions $\phi(\alpha_j)$ are not zero.

104. Most of the properties of ordinary Riemann matrices belong also to those of the domain $K(\alpha_j)$. Let us indicate a few of them as well as their corollaries for Ω.

Assume that there exist $1 + k_1$ linearly independent complexes such as (16), say

$$\sum_{\mu,\nu}^{1\cdots 2p'} \gamma^s_{\mu\nu}(\alpha_j)\, x_\mu y_\nu = 0 \qquad (\gamma^s_{\mu\nu} = -\gamma^s_{\nu\mu}),$$

belonging to Ω. The equations in the coefficients $c^{mn}_{\mu\nu}$ of the alternate forms of Ω, analogous to the equations (14), become

$$\sum_{m,n}^{1\cdots q} c^{mn}_{\mu\nu}\, \alpha_j^{m-1}\, \alpha_h^{n-1} = 0 \qquad (\alpha_j \neq \alpha_h)$$

$$\sum_{m,n}^{1\cdots q} c^{mn}_{\mu\nu}\, \alpha_j^{m+n-2} = \sum_{s=1}^{1+k_1} \phi_s(\alpha_j)\, \gamma^s_{\mu\nu}(\alpha_j),$$

where the (ϕ)'s are polynomials with rational coefficients. They show that

$$1 + k = q(1 + k_1).$$

Similarly if there are $1 + h_1$ reciprocities

$$\sum_{\mu,\nu}^{1\cdots 2p'} \gamma^s_{\mu\nu}(\alpha_j)\, x_\mu\, y_\nu = 0,$$

then $1 + h = q(1 + h_1)$.

The matrix Ω will be pure if it does not possess any other bilinear forms of the type just defined (this we have tacitly assumed in the above formulas)—and if moreover none of these forms are degenerate.

We may apply to the matrices τ_j a transformation defined by the symbolic matrix-equation:

$$\tau'_j = \tau_j \cdot \| \beta_{\mu\nu}(\alpha_j) \| \qquad (\mu, \nu = 1, 2, \cdots, 2p'),$$

where the (β)'s are numbers of the domain $K(\alpha_j)$. Then we may apply to τ_j a linear transformation of the rows. If we do this simultaneously for every

τ_j we have a transformation of isomorphism of Ω. The matrices τ_j must be considered as impure if, for every j,

$$\tau'_j \equiv \left\| \begin{matrix} \tau_1^j, & 0, & \cdots, & 0 \\ 0, & \tau_2^j, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots, & \tau_n^j \end{matrix} \right\|$$

where τ_h^j is a matrix with p'_h rows and $2p'_h$ columns, p'_h being independent of j. In this case Ω is isomorphic to a matrix of type (I), the submatrices ω_i being invariant under the Riemann projectivity considered. Such a condition will certainly arise if $1 + h_1 > 2p'$. In all cases, as Scorza showed for ordinary Riemann matrices, we have

$$1 + h_1 \leqq 2p'^2, \qquad 1 + k_1 \leqq p'^2,$$

hence

$$1 + h \leqq pr, \qquad 1 + k \leqq \tfrac{1}{2}pr.$$

When the indices h_1, k_1 have their maximum values, Ω is isomorphic to a matrix composed with an array τ such that

$$\tau_j \equiv \left\| \begin{matrix} 1, & \delta(\alpha_j), & 0, & 0, & \cdots, & 0 \\ 0, & 0, & 1, & \delta(\alpha_j), & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \cdot & \cdot & 1, & \delta(\alpha_j) \end{matrix} \right\|$$

where $\delta(\alpha_j)$ is a quadratic number of the domain $K(\alpha_j)$ (Scorza).

The numbers h_1, k_1 may have lacunary values and they can be obtained as those of h, k have been obtained by Scorza.

If $h_1 > 0$, then there exists at least one complex multiplication T' permutable with the multiplication T whose multipliers are the (α)'s. There will then be a multiplication of degree $q' \geqq 2q$ permutable with both T and T' and we can investigate Ω by taking this multiplication as a starting point. But there may be advantage in considering directly the Riemann projectivities of τ_j, and if Ω is pure τ_j may be composed with two matrices

$$\| \theta_{k1}^j, \quad \theta_{k2}^j, \quad \cdots, \quad \theta_{kr}^j \|, \qquad \| 1, \quad \beta_{jk}, \quad \beta_{jk}^2, \quad \cdots, \quad \beta_{jk}^{q'-1} \|$$

where the numbers β_{jk} are roots of an irreducible equation $f(\beta) = 0$ of degree $q' = 2p'/r'$ with coefficients in the same domain as already considered.

Let Ω' be another Riemann matrix of genus p possessing a Riemann projectivity having also $f(\alpha) = 0$ for characteristic equation and assume Ω and Ω' both pure. They will be isomorphic if there exists a simultaneous form

$$\sum \gamma_{\mu\nu}(\alpha_j)\, x_\mu\, y_\nu$$

which vanishes when the (x)'s are replaced by the elements of any row of τ_j

and the (y)'s by those of any row of τ_j' which corresponds to τ_j for Ω', this for $j = 1, 2, \cdots, p'$. If there exist λ_1 such forms, the simultaneous index of Ω, Ω' is $\lambda = q\lambda_1$.

In concluding, let us remark that the arithmetic properties of alternate forms belonging to ordinary Riemann matrices can be extended at once to those which we have here considered. For these propositions can in general be derived by purely arithmetic methods and without mentioning Abelian varieties at all. For example, the theorems given by Cotty in his thesis, on hyperelliptic surfaces and the corresponding forms, can be at once extended to τ_j when $r = 2p' = 4$.

105. *Real multipliers* $(r = 2p' = 2)$. When $r = 2$ and $\alpha_1, \alpha_2, \cdots, \alpha_p$ include all the roots of $f(\alpha) = 0$ they must necessarily be real, at least when the array τ is as general as possible. For if

$$\sum_{\mu, \nu}^{1,2} \gamma_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu \tag{18}$$

is an alternate form of Ω, it is necessary that $\gamma_{\mu\nu}(\alpha_j, \alpha_k) = 0$ if $\alpha_j \neq \alpha_k$, hence $\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) = 0$ if $\alpha_j \neq \bar{\alpha}_j$, and these matrices exist only if the (α)'s are all real. They are then of the type of matrices which we have just investigated. We may always arrange matters so that no τ_{j1} will be zero. If we divide then every term in the j-th row of Ω by τ_{j1}, the array τ will assume the form

$$\| 1, \tau_j \| \qquad (j = 1, 2, \cdots, p).$$

The arbitrary constants τ_j must be imaginary else Ω would have a row with elements all real. If the form (18) is an alternate form of Ω,

$$\gamma_{\mu\nu}(\alpha_j, \alpha_k) = -\gamma_{\nu\mu}(\alpha_k, \alpha_j), \qquad \gamma_{\mu\nu}(\alpha_j, \alpha_k) = 0 \text{ if } \alpha_k \neq \alpha_j;$$
$$\gamma_{\mu\nu}(\alpha_j, \alpha_j) \neq 0;$$

and hence $1 + k = q$. If on the contrary (18) is not an alternate form of Ω, and if the parameters τ_j remain entirely arbitrary it is necessary that

$$\gamma_{\mu\mu}(\alpha_j, \alpha_k) = 0 \quad (\mu = 1, 2); \ \gamma_{12}(\alpha_j, \alpha_k) = \gamma_{21}(\alpha_j, \alpha_k) = 0 \text{ if } \alpha_j \neq \alpha_k;$$

$$\gamma_{12}(\alpha_j, \alpha_j) = -\gamma_{21}(\alpha_j, \alpha_j);$$

whence again $1 + h = q = p = 1 + k$.

Assume that (18) is an alternate form of Ω. The polynomial

$$\gamma(\alpha) = \gamma_{12}(\alpha, \alpha)$$

is after all merely an arbitrary polynomial of degree $q - 1$. The Hermitian form corresponding to (18) is

$$-\frac{1}{2i}\sum_{j=1}^{p} \gamma(\alpha_j)(\bar{\tau}_j - \tau_j) x_j \bar{x}_j = \sum_{j=1}^{p} \gamma(\alpha_j) \tau_j'' x_j x_j \qquad (\tau_j = \tau_j' + i\tau_j'').$$

We can always take $\gamma(\alpha)$ such that the coefficients will all be positive, hence whatever the parameters τ_j, Ω is always a Riemann matrix. If we assume, as we have done so far, that $f(\alpha)$ is irreducible, then when one of the numbers $\gamma(\alpha_j)$ is zero they will all be. Since moreover none of the τ_j'' can be zero, whenever Ω possesses no other alternate forms than those of the above type, the Hermitian form is always of genus p and Ω is pure.

Can the matrix be pure and possess a new Riemann projectivity? In order that this be the case it must possess a bilinear form other than of the above type, say

$$\sum_{\mu,\nu}^{1,2} \beta_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu,$$

imposing some relations between the parameters τ_j. Two cases are possible: (*a*) The expressions $\beta_{\mu\nu}(\alpha_j, \alpha_k)$ $(\alpha_j \neq \alpha_k)$ are all zero, but the $\beta_{\mu\nu}(\alpha_j, \alpha_j)$ are not. There will then be no new alternate form, hence $1 + h = 2p$, $1 + k = p$. The new complex multiplication is permutable with the former. The matrix Ω which is still pure possesses a Riemann projectivity with irreducible characteristic equation and we fall back upon the case studied in § 2. This is a consequence of the fact that the reciprocity

$$\sum_{\mu,\nu}^{1,2} \beta_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu = 0$$

leaves the point $(1, \tau_j)$ invariant, hence the parameters τ are then quadratic conjugate numbers of the real domains $K(\alpha_j)$. The matrix Ω is then isomorphic to a matrix with array τ of type $\| 1, \sqrt{R(\alpha_j)} \|$, where $R(\alpha_j)$ is an integer of the same domain, negative together with all its conjugates. (*b*) The expressions $\beta_{\mu\nu}(\alpha_j, \alpha_k)$ $(\alpha_j \neq \alpha_k)$ are not all zero. In this case $1 + h = q + q(q-1) = p^2 > 2p$ if $p > 2$. Hence Ω is impure if $p > 2$. Thus if $r = 2$ and if the multipliers are all real, Ω if pure cannot possess more than two other Riemann projectivities, one of degree two and the other of degree $2p$, permutable with the given one.

106. *Imaginary multipliers.* We shall first consider a question concerning Hermitian forms.

Given the Hermitian form of genus r

$$\sum_{\mu=1}^{r} a_\mu x_\mu \bar{x}_\mu,$$

let $S_{r'-1}$, $S_{r''-1}$ be two spaces of S_r such that $r' + r'' = r$ and conjugated with respect to the reciprocity

$$\sum a_\mu x_\mu y_\mu = 0.$$

Under what conditions can the Hermitian form be positive at all points of the

first space and negative at all points of the second? The equations of $S_{r'-1}$ can be put in the form

$$x_{r'+\nu} = \sum_{\mu=1}^{r'} b_{\nu\mu}\, x_\mu \qquad (\nu = 1, 2, \cdots, r''),$$

and it will be necessary that

$$\sum_{\mu=1}^{r'} a_\mu\, x_\mu\, \bar{x}_\mu + \sum_{\nu=1}^{r''} a_{r'+\nu} \Big(\sum_{\mu=1}^{r'} b_{\nu\mu}\, x_\mu \Big) \Big(\sum_{\mu=1}^{r'} \bar{b}_{\nu\mu}\, \bar{x}_\mu \Big) > 0 .$$

This expression can certainly be made negative if it is possible to annul all the terms whose coefficients a_μ are positive without annulling the others. Let s' be the number that are positive and s'' the remaining. We shall have s' linear equations in r' unknowns and since they must not have any solutions, it is necessary that $r' \leqq s'$. Similarly we must have $r'' \leqq s''$, but $r' + r'' \geqq s' + s''$; hence $r' = s'$, $r'' = s''$. These conditions are besides sufficient. To see it we may consider the form

$$\sum_{\mu=1}^{r'} \bar{x}_\mu\, x_\mu - \sum_{\nu=1}^{r''} x_{r'+\nu}\, \bar{x}_{r'+\nu}$$

and the two conjugate spaces

$$\begin{aligned} &S_{r'-1}\,; \quad x_{r'+\nu} = \lambda_\nu\, x_1 && (\nu = 1, 2, \cdots, r''), \\ &S_{r''-1}; \quad x_2 = x_3 = \cdots = x_{r'} = 0, && x_1 = \sum_{\nu=1}^{r''} \lambda_\nu\, x_\nu , \end{aligned}$$

where the (λ)'s satisfy the conditions

$$\sum \lambda_\nu \bar{\lambda}_\nu < 1 .$$

On $S_{r'-1}$ the Hermitian form becomes

$$\Big(1 - \sum \lambda_\nu \bar{\lambda}_\nu\Big) x_1\, \bar{x}_1 + \sum_{\mu=2}^{r'} x_\mu\, \bar{x}_\mu$$

and its sign is $+$. On $S_{r''-1}$ it reduces to

$$\begin{aligned} &\sum_{\nu=1}^{r''} \lambda_\nu\, x_{r'+\nu} \sum_{\nu=1}^{r''} \bar{\lambda}_\nu\, \bar{x}_{r'+\nu} - \sum_{\nu=1}^{r''} x_{r'+\nu}\, \bar{x}_{r'+\nu} \\ &\qquad = \Big| \sum \lambda_\nu\, x_{r'+\nu} \Big|^2 - \sum x_{r'+\nu}\, \bar{x}_{r'+\nu} \\ &\qquad < \Big(\sum |\lambda_\nu\, x_{r'+\nu}| \Big)^2 - \sum |x_{r'+\nu}|^2 < \sum |\lambda_\nu|^2 \sum |x_{r'+\nu}|^2 - \sum |x_{r'+\nu}|^2 \\ &\qquad = \Big(-1 + \sum \bar{\lambda}_\nu \lambda_\nu \Big) \sum |x_{r'+\nu}|^2 < 0 , \end{aligned}$$

as was desired. This shows also that there is an infinity of pairs of spaces answering the question.

107. We now pass to the study of matrices with imaginary multipliers. We shall limit ourselves to the case *where the group G of the equation $f(\alpha) = 0$ is permutable with the unique operation that permutes each root with its conjugate.* I say that in this case if there exists a form (12) satisfying only the conditions

(a) and (c''), Ω is a Riemann matrix. For let $\sum \beta_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu$ be a form answering the question. We may determine polynomials with rational coefficients and of degree $q-1$ in α_j, α_k, say $\gamma_{\mu\nu}(\alpha_j, \alpha_k)$, by the relations

$$\begin{aligned}\gamma_{\mu\nu}(\alpha_j, \alpha_k) &= 0 \qquad \text{if} \qquad \alpha_j \neq \alpha_k;\\ \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) &= \beta_{\mu\nu}(\alpha_j, \bar{\alpha}_j).\end{aligned}$$

That this is possible in view of the property assumed for the group of $f(\alpha) = 0$ follows from § 2, and we see then that the form

$$\sum \gamma_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu \tag{19}$$

is a Riemann form of Ω. For, the spaces S_{r_j-1}, S_{r_k-1} will be conjugated with respect to the proper reciprocity, in particular S_{r_j-1}, $S_{r'_j-1}$ with respect to

$$\sum \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) x_\mu y_\nu = 0 \tag{20}$$

and the Hermitian forms

$$-\frac{1}{2i} \sum \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) x_\mu \bar{x}_\nu \tag{21}$$

will be positive at all points of S_{r_j-1} and negative at all points of $S_{r'_j-1}$. As the Hermitian form belonging to (19) is here the sum of the forms (21) it is definite positive, and Ω is effectively a Riemann matrix.

108. To establish the existence of matrices of the type considered it is sufficient to show that we can take polynomials with rational coefficients $\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j)$, such that when the Hermitian form

$$-\frac{1}{2i} \sum \gamma_{\mu\nu} x_\mu \bar{x}_\nu$$

is reduced to the type

$$\sum \gamma_\mu x_\mu \bar{x}_\mu,$$

r_j coefficients γ_μ are positive and r'_j negative. This is equivalent to requiring that of the r roots of the equation in γ (all real, as is well-known),

$$\left| -\frac{1}{2i} \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j) - \epsilon_{\mu\nu} \cdot \gamma \right| = 0 \qquad (\epsilon_{\mu\mu} = 1;\ \epsilon_{\mu\nu} = 0,\ \mu \neq \nu),$$

r_j be positive and r'_j negative. Indeed, we can then determine polynomials with rational coefficients $\gamma'_{\mu\nu}(\alpha_j, \alpha_k)$ such that

$$\gamma'_{\mu\nu}(\alpha_j, \alpha_k) = 0 \quad \text{if} \quad \alpha_j \neq \alpha_k; \qquad \gamma'_{\mu\nu}(\alpha_j, \bar{\alpha}_j) = \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j),$$

and also spaces S_{r_j}, $S_{r'_j-1}$ satisfying the conditions (a), (c'') relatively to

$$\sum \gamma'_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu,$$

and there will therefore exist a Riemann matrix belonging to $f(\alpha) = 0$ and to the distribution $\alpha_1, \alpha_2, \cdots, \alpha_p$ of its roots.

Now let us take rq numbers $\eta_{j\mu}$ such that with $\alpha_{j'} = \overline{\alpha}_j$,

$$\eta_{j,\,1} = \eta_{j,\,2} = \cdots = \eta_{j,\,r_j} = +1; \qquad \eta_{j,\,r_j+1} = \cdots = n_{j,\,r} = -1;$$
$$\eta_{j',\,1} = \eta_{j',\,2} = \cdots = \eta_{j',\,r_j} = -1; \qquad \eta_{j',\,r_j+1} = \cdots = \eta_{j',\,r} = +1,$$

and consider the equations

$$-\frac{1}{2i}\sum_{m,n}^{1\cdots q} c_{\mu\nu}^{mn}\left(\alpha_j^{m-1}\,\overline{\alpha}_j^{n-1} - \overline{\alpha}_j^{m-1}\,\alpha_j^{n-1}\right) = \eta_{j\mu} \qquad (j = 1, 2, \cdots, q;\ \mu = 1, 2, \cdots, r),$$

of which we shall take a type solution in real numbers $c_{\mu\nu}^{mn}$. Designate then by $-\frac{1}{2i}\,\delta_{\mu\mu}(\alpha_j, \overline{\alpha}_j)$ the left-hand sides. The equation in γ

$$\left| -\frac{1}{2i}\,\delta_{\mu\nu}(\alpha_j, \overline{\alpha}_j) - \epsilon_{\mu\nu}\cdot\gamma \right| = 0 \qquad (\epsilon_{\mu\nu} = \delta_{\mu\nu} = 0,\ \mu \neq \nu;\ \epsilon_{\mu\mu} = 1),$$

has r_j positive and r_j' negative roots, this for $j = 1, 2, \cdots, q$, all equal to unity in absolute value. Let us take finally polynomials $\gamma_{\mu\nu}(\alpha_j, \overline{\alpha}_j)$ with rational coefficients differing as little as we please from those of the (δ)'s. The Hermitian form

$$-\frac{1}{2i}\sum \gamma_{\mu\nu}(\alpha_j, \overline{\alpha}_j)\, x_\mu\, \bar{x}_\nu$$

will obviously answer the question. The existence of our matrices is therefore proved and at the same time we have given a construction for them.

To obtain h, τ being assumed as general as possible, we remark that the number of independent relations

$$\sum_{m,n}^{1\cdots q} b_{mn}\,\alpha_j^{m-1}\,\overline{\alpha}_j^{n-1} = 0 \qquad (j = 1, 2, \cdots, q)$$

is equal to the number of independent solutions for the (b)'s, that is, to $q(q-1)$. Hence $t' = q$. Similarly for k we must consider the number of relations

$$\sum_{m,n}^{1\cdots q} b_{mn}\left(\alpha_j^{m-1}\,\overline{\alpha}_j^{n-1} + \overline{\alpha}_j^{m-1}\,\alpha_j^{n-1}\right) = 0 \qquad (j = 1, 2, \cdots, \tfrac{1}{2}q).$$

This number is $\frac{1}{2}q^2$, hence

$$t = \frac{q(q+1)}{2} - \tfrac{1}{2}q^2 = \tfrac{1}{2}q.$$

It follows that

$$1 + h = 2(1 + k) = q + 2r^2\left[\binom{q}{2} - s\right].$$

This assumes $r > 2$. When $r = 2$ and the numbers r_j are not all equal to unity, nothing is changed. If they are all equal to unity we must add q alternate forms to h and k (the same forms as occur in the case of real multi-

pliers), and since $s = \binom{q}{2}$, we have

$$1 + h = 2q, \qquad 1 + k = \tfrac{3}{2}q.$$

Remark: When $f(\alpha) = 0$ is Abelian, it becomes possible to determine s. For it is certainly possible to derive from the set $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ all the pairs of roots by the operations of G if the number of distinct multipliers exceeds $\frac{1}{2}q$ (No. 91). Hence when this occurs, as it does in the most general case, we have $s = \binom{q}{2}$, and therefore $1 + h = 2(1 + k) = q$, with the added condition that if $r = 2$ the multipliers must not all be distinct. When they are we are thrown back on the formulas already derived for this special case.

Assume now that there are exactly $\frac{1}{2}q$ distinct multipliers. Then (No. 84) Ω is impure of type (II) composed r times with

$$\omega \equiv \| 1, \alpha_j, \cdots, \alpha_j^{q-1} \| \qquad (j = 1, 2, \cdots, \tfrac{1}{2}q)$$

which is itself pure or impure according as the subgroup G' of G which maintains invariant the set $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ does or does not reduce to the identity. Let n be the order of G'. The invariants of ω are given by $1 + h' = 2(1 + k') = nq$ and those of Ω by $1 + h = 2(1 + k) = nr^2 q = nrp$.

109. The form in the left-hand side of (20) can be reduced to one of the same nature with $\gamma_{\mu\nu}(\alpha_j, \overline{\alpha}_j) = 0 \quad (\mu \neq \nu)$, by a transformation of variables

$$x'_\mu = \sum_\nu b_{\mu\nu}(\alpha_j, \overline{\alpha}_j) x_\nu, \qquad y'_\mu = \sum_\nu b_{\mu\nu}(\overline{\alpha}_j, \alpha_j) y_\nu,$$

where the (b)'s are as before polynomials with rational coefficients. Now according to what has been stated in No. 89, these equations can be put in the simple form

$$x'_\mu = \sum_\nu e_{\mu\nu}(\alpha_j) x_\nu, \qquad y'_\mu = \sum_\nu e_{\mu\nu}(\overline{\alpha}_j) y_\nu,$$

where the (e)'s are still polynomials with rational coefficients. This is all equivalent to stating that Ω can be transformed into an isomorphic matrix for which (20) is replaced by $\sum_{\mu=1} \gamma_{\mu\mu}(\alpha_j, \overline{\alpha}_j) x_\mu y_\mu$. Moreover

$$\gamma_{\mu\mu}(\alpha_j, \overline{\alpha}_j) = (\alpha_j - \overline{\alpha}_j) \sum c_{\mu\mu}^{mn} (\alpha_j^m \overline{\alpha}_j^n + \overline{\alpha}_j^m \alpha_j^n)$$

and contains therefore $\frac{1}{2}q$ arbitrary coefficients. Hence Ω depends upon $\frac{1}{2}rq = p$ arbitrary integers and upon $\frac{1}{2}\sum_{j=1}^{j=q} r_j r'_j$ continuous essential parameters, namely the parameters which determine the position of one of the spaces S_{r_j-1}, $S_{r'_j-1}$ for each pair of roots $(\alpha_j, \overline{\alpha}_j)$.

When there are no other alternate forms than those derived from (19), Ω is pure since the Hermitian form belonging to each alternate form is the sum of q forms of genera r_j, with independent variables, hence its genus is $\sum r_j = p$. This is still true if there are $1 + k_0$ forms of the type in question,

such that the corresponding forms (20)

$$\sum \gamma^{s}_{\mu\nu}(\alpha_j, \bar{\alpha}_j) x_\mu y_\nu \qquad (s = 1, 2, \cdots, 1 + k_0)$$

are linearly independent and moreover do not possess any combination with coefficients polynomials in α_j, $\bar{\alpha}_j$, degenerate. In all cases if $r > 2$, or $r = 2$, and the multipliers are not all distinct, $1 + k = \frac{1}{2}q(1 + k_0)$, and in the same conditions if there are h_0 non-alternate forms of the same type,

$$1 + h = q(1 + h_0).$$

When the multipliers are all distinct $1 + k$ is the same, but $1 + h = q(2 + h_0)$.

Let us consider a little more closely the case just mentioned where Ω possesses two bilinear forms of type (19) with forms (20) independent. Let A_j, B_j be the reciprocities determined by two of them between the spaces S_{r_j-1}, $S_{r'_j-1}$. Then $A_j^{-1}\cdot B_j$ is a projectivity transforming S_{r_j} into itself. It is defined by equations such as $x'_\mu = \sum_\nu b_{\mu\nu}(\alpha_j, \bar{\alpha}_j) x_\nu$, which as before can be put in the form $x'_\mu = \sum_\nu e_{\mu\nu}(\alpha_j) x_\nu$, and it is readily seen that these relations define, as in the case of real roots, a complex multiplication permutable with the multiplication whose multipliers are the (α)'s.

Remark: Let us assume that the integers r_j are all equal and that moreover Ω possesses an alternate form (19) such that $\gamma_{\mu\nu}(\alpha_j, \alpha_k) = 0$ if $\alpha_j \neq \alpha_k$. It will then be possible to apply with scarcely any change everything that has been said in the case of real multipliers. However h and k will not be the same. Let there be k_1 forms of the nature in question and such that the alternate forms

$$\sum \gamma^{s}_{\mu\nu}(\alpha_j, \alpha_j) x_\mu y_\nu \qquad (s = 1, 2, \cdots, k_1),$$
$$\gamma^{s}_{\mu\nu}(\alpha_j, \alpha_j) = -\gamma^{s}_{\nu\mu}(\alpha_j, \alpha_j)$$

are linearly independent. We will then have

$$1 + h = \tfrac{1}{2}(1 + k_0 + 2k_1) + r^2\left[\binom{q}{2} - s\right].$$

Similarly if there are h_1 non-alternate forms, then

$$1 + h = q(1 + h_0 + h_1) + 2r^2\left[\binom{q}{2} - s\right].$$

110. Can Ω possess a new bilinear form

$$\sum \delta_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu \tag{22}$$

without possessing other alternate forms than those derived from (19)? In order that this be the case, it is necessary that the following relations be verified:

$$\delta_{\mu\nu}(\alpha_j, \alpha_k) - \delta_{\nu\mu}(\alpha_k, \alpha_j) = 0,$$
$$(\alpha_j - \alpha_k)[\delta_{\mu\nu}(\alpha_j, \alpha_k) + \delta_{\nu\mu}(\alpha_k, \alpha_j)] = 0 \qquad \text{if} \qquad \alpha_j \neq \bar{\alpha}_k,$$
$$\delta_{\mu\nu}(\alpha_j, \bar{\alpha}_j) - \delta_{\nu\mu}(\bar{\alpha}_j, \alpha_j) = \phi(\alpha_j, \bar{\alpha}_j)\cdot\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j),$$
$$(\alpha_j - \bar{\alpha}_j)[\delta_{\mu\nu}(\alpha_j, \bar{\alpha}_j) + \delta_{\nu\mu}(\bar{\alpha}_j, \alpha_j)] = \psi(\alpha_j, \bar{\alpha}_j)\cdot\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j).$$

From the first two we conclude that

$$\delta_{\mu\nu}(\alpha_j, \alpha_k) = 0 \quad \text{if} \quad \alpha_j \neq \alpha_k \text{ or } \bar{\alpha}_k,$$
$$\delta_{\mu\nu}(\alpha_j, \alpha_j) = \delta_{\nu\mu}(\alpha_j, \alpha_j),$$

and from the last two that

$$\delta_{\mu\nu}(\alpha_j, \bar{\alpha}_j) = \chi(\alpha_j, \bar{\alpha}_j)\cdot\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j).$$

This shows that we may combine the two forms (19) and (22) so as to obtain a form

$$\sum \zeta_{\mu\nu}(\alpha_j, \alpha_k)\, x_\mu\, y_\nu$$

such that $\zeta_{\mu\nu}(\alpha_j, \alpha_k) = 0$ if $\alpha_j \neq \alpha_k$, while

$$\sum \zeta_{\mu\nu}(\alpha_j, \alpha_j)\, x_\mu\, y_\nu = 0$$

represents a quadric of S_{r-1} which must contain the space S_{r_j-1}. If this quadric were degenerate Ω would possess a degenerate bilinear form and would therefore be impure. Limiting ourselves to the case of pure matrices, we must then have $r_j - 1 \leqq \frac{1}{2}(r-2)$ when r is even and $r_j - 1 \geqq \frac{1}{2}(r-3)$ when it is odd (Bertini). Similar limits hold of course for $r_j' - 1$. But $r_j + r_j' = r$, hence r must be even and we must have besides $r_j = r_j' = \frac{1}{2}r$. Thus r must be even, and among the multipliers each root must be taken the same number of times. In this case the solution exists actually as can be shown by the following choice of bilinear forms: For (19) we take a form such that $\gamma_{\mu\nu}(\alpha_j, \alpha_k) = 0$ if $\alpha_j \neq \alpha_k$ and

$$-\frac{1}{2i}\sum \gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j)\, x_\mu\, y_\nu = \sum_{\mu=1}^{r/2} \left(x_\mu\, y_\mu - x_{\frac{r}{2}+\mu}\, y_{\frac{r}{2}+\mu}\right);$$

for the quadric (22) we take

$$\sum_{\mu=1}^{r/2} x_\mu\, x_{\frac{r}{2}+\mu} = 0;$$

and for the spaces S_{r_j-1}, $S'_{r_j'-1}$,

$$S_{r_j-1}\colon x_{\frac{r}{2}+\mu} = 0, \qquad S'_{r_j'-1}\colon x_\mu = 0$$

$$(\mu = 1, 2, \cdots, r/2), \qquad (j = 1, 2, \cdots, q/2), \qquad \alpha_h \neq \alpha_k \text{ if } h, k \leqq q/2.$$

If there are two non-degenerate reciprocities such as (22), the product of one by the inverse of the other defines a new multiplication permutable with the first. Ω possesses then a complex multiplication of degree $q' \geqq 2q$, and we have $1 + k > \frac{1}{4}(2q) = \frac{1}{2}q$, hence there must be a new alternate form. In other words, the existence of two such reciprocities increases necessarily the index of singularity, k. When there is only one we have

$$1 + k = \tfrac{1}{2}q; \qquad 1 + h = 2q.$$

111. As an application we shall establish the existence of non-singular Abelian varieties with complex multiplication whose existence has recently been announced without proof by Scorza.*

According to No. 101 we must have $q = 2$ and the characteristic equation of the complex multiplication in question must be of the type

$$(a\alpha^2 + b\alpha + c)^q = 0, \qquad b^2 < 4ac,$$

with $p > 2$. We then have $1 + h = 2$, $1 + k = 1$ and it is sufficient to construct the matrices such as those of Nos. 107, 108 corresponding to this complex multiplication. We may observe that among the multipliers one of the roots may be taken any number of times $< p$. When p is even there exist varieties with two complex multiplications such as those of No. 111, and for them $1 + h = 4$, $1 + k = 1$. According to what we have just seen, if there is one more reciprocity of this type we have certainly $k > 0$. The matrices in question are therefore the only non-singular matrices with complex multiplication.

This result may be extended to varieties with a complex multiplication whose multipliers are real and to multiplications permutable with these. The integers h_0, k_0 having always the same meaning as previously we find that for $k_1 = 0$, h_1 can only take the values 0, 1, 3. Finally it is easy to construct the corresponding matrices—by merely replacing everywhere the ordinary domain of rationality by the domain $K(\alpha_j)$—but we shall not dwell on this any further.

This ends the discussion of complex multiplications. We shall proceed to make a rapid application to the classification of pure matrices for $p = 2$ or 3.

§6. Pure matrices of genus two or three

112. *Matrices of genus two.* If a matrix of genus two is singular and pure, it must possess a Riemann projectivity whose characteristic equation is of type $[f(\alpha)]^r = 0$, ($f(\alpha)$ irreducible). Since $rq = 4$, r can only have the values 1, 2. Let first $r = 1$. We have seen in No. 89 that Ω is then reducible to the type

$$\left\| \begin{matrix} 1, & \alpha_1, & \alpha_1^2, & \alpha_1^3 \\ 1, & \alpha_2, & \alpha_2^2, & \alpha_2^3 \end{matrix} \right\|,$$

where α_1, α_2 are roots of an equation of degree four

$$(\alpha^2 - 2\zeta_1\alpha + m\zeta_1 + n)(\alpha^2 - 2\zeta_2\alpha + m\zeta_2 + n) = 0$$

with m, n rational and ζ_1, ζ_2 roots of an equation

$$a\zeta^2 + b\zeta + c = 0,$$

*Comptes Rendus, October, 1917. (Added in 1922: The proof has since been supplied in his memoir of the Palermo Rendiconti, vol. 45 (1921), p. 185. It appears to be decidedly different from ours.)

and we have indicated there the conditions that a, b, c, m, n must satisfy. As to the invariants of Ω, they are $1 + h = 2(1 + k) = 4$.

113. Let now $r = 2$ and assume the multipliers real. The matrix Ω is isomorphic to a matrix composed with two arrays

$$\left\| \begin{matrix} 1, & \tau_1 \\ 1, & \tau_2 \end{matrix} \right\|, \qquad \left\| \begin{matrix} 1, & \sqrt{d} \\ 1, & -\sqrt{d} \end{matrix} \right\|,$$

where d is a positive integer not a perfect square. We know that Ω exists provided τ_1, τ_2 are imaginary. Just by way of illustration we give the calculation, which is here very simple. There will be an alternate form

$$\gamma_{12}(\sqrt{d}, -\sqrt{d})\, x_1 y_2 + \gamma_{21}(\sqrt{d}, -\sqrt{d})\, x_2 y_1$$

with

$$\gamma_{12}(x, y) = -\gamma_{21}(y, x) = \lambda(xy + d) + \mu(x + y),$$

so chosen as not to impose any condition on τ_1 and τ_2. This form contains two arbitrary parameters, hence $1 + k = 2$, and similarly $1 + h = 2$ as we already knew. The corresponding Hermitian form is, up to the factor $\sqrt{d}$,

$$\tau''(\mu + \lambda\sqrt{d})\, x_1 \bar{x}_1 - \tau_1''(\mu - \lambda\sqrt{d})\, x_2 \bar{x}_2; \qquad \tau_j = \tau_j' + i\tau_j''.$$

We must therefore have

$$\tau_1''(\mu + \lambda\sqrt{d}) > 0, \qquad \tau_2''(\mu - \lambda\sqrt{d}) < 0.$$

We can always assume that one of the numbers τ_1'', τ_2'' is positive—say τ_1''. The existence of Ω is certain for we can take λ, μ positive and such that $\mu - \lambda\sqrt{d}$ has the sign of $-\tau_2''$. Moreover the matrix is pure because the Hermitian form is of genus two provided that λ and μ are not both zero. The sets of integers (λ, μ) satisfying the above equalities define the principal forms and therefore also the systems of Abelian functions corresponding to the matrix.

If there exists a non-alternate bilinear form imposing some relations upon τ_1, τ_2, these numbers are conjugate quadratic numbers of the domain $K(\sqrt{d})$, and Ω possesses a Riemann projectivity with irreducible characteristic equation. It is therefore of the type considered in No. 112.

114. Let us pass to the case of complex multipliers. We have now two arrays

$$\left\| \begin{matrix} 1, & \tau_1 \\ 1, & \tau_2 \end{matrix} \right\|, \qquad \left\| \begin{matrix} 1, & i\sqrt{d} \\ 1, & -i\sqrt{d} \end{matrix} \right\|,$$

where d is as before a positive integer not a perfect square. From the existence of an alternate form, follows a bilinear relation between τ_1 and τ_2, whose coefficients belong to the domain $K(i\sqrt{d})$. If Ω is pure we can always reduce it to an isomorphic matrix composed with two similar arrays such that

the relation in question is then $c_{11} - c_{22}\,\tau_1\,\tau_2 = 0$, where c_{11}, c_{22} are integers. The corresponding Hermitian form is

$$c_{11}\,x_1\,\bar{x}_1 - c_{22}\,x_2\,\bar{x}_2\,.$$

It must be positive for $x_1 = 1$, $x_2 = \tau_1$, and negative for $x_1 = 1$, $x_2 = \tau_2$. It follows that c_{11}, c_{22} must have the same signs and that their ratio must be included between $\tau_1\,\bar{\tau}_1$ and $\tau_2\,\bar{\tau}_2$, numbers which must not be equal. This is equivalent to the sole condition $|\tau_1| \neq |\tau_2|$. The invariants of Ω are $1 + h = 4, 1 + k = 3$. As they have the maximum value for a pure matrix, Ω cannot acquire any other bilinear forms. This completes the discussion of the case $p = 2$.

We see that for a pure matrix of genus 2, the only possible combinations (h, k) are $(0, 0)$, $(1, 1)$, $(3, 2)$, and $(3, 1)$. The corresponding matrices depend respectively upon 3, 2, 1, 0 continuous parameters.

115. *Matrices of genus three.* When $p = 3$, $qr = 6$; hence $r = 1$, 2, or 3. Let first $r = 1$, and therefore $q = 3$. The characteristic equation is

$$\prod_{j=1}^{3}(\alpha^2 - 2\zeta_j\,\alpha + \lambda\zeta_j^2 + \mu\zeta_j + \nu) = 0,$$

where the (ζ)'s are roots of an irreducible equation $\zeta^3 + p\zeta^2 + q\zeta + r = 0$. Let T be an operation of the group G of the characteristic equation, permuting cyclically the pairs $(\alpha_1, \bar{\alpha}_1)$, $(\alpha_2, \bar{\alpha}_2)$, $(\alpha_3, \bar{\alpha}_3)$. It corresponds to the cyclic operation of order 3 that the group of the equation in ζ always contains. If we observe that T is permutable with the binary operation S of G permuting pairs of conjugate roots, we see that with a suitable choice of notation T has one of the following two forms:

$$(\alpha_1, \alpha_2, \alpha_3)\cdot(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3); \qquad (\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3).$$

Hence G always contains a cyclic subgroup of order 6, of the powers of TS in the first case and of the powers of T in the second. This is sufficient to allow us to affirm, as in the case of an Abelian equation, that there exists a pure matrix corresponding to the above equation since it will always be possible to choose three roots α_1, α_2, α_3 of which none are conjugate to each other and such that from the pairs (α_1, α_2), (α_2, α_3), (α_3, α_1) we may deduce, by the operations of the group, every pair of non-conjugate roots. As to the invariants, they will have the values $1 + h = 2(1 + k) = 6$.

116. Let us assume now $r = 2$. The matrix Ω is then composed with the arrays

$$\|\,\tau_{j1},\,\tau_{j2}\,\|, \qquad \|\,1,\,\alpha_j,\,\alpha_j^2\,\| \qquad (j = 1, 2, 3),$$

the multipliers being the roots of an equation of the third degree. I say that in order that Ω be pure, these roots must all be real. For if $\sum\gamma_{\mu\nu}\,(\alpha_j, \alpha_k)\,x_\mu\,y_\nu$

is a principal form, the corresponding Hermitian form will be definite only if its coefficients A_{jj} are not all zero, which requires that the quantities $\gamma_{\mu\nu}(\alpha_j, \bar{\alpha}_j)$ $(\mu, \nu = 1, 2, 3, 4)$ be not all zero. Hence, if there is a pair of imaginary multipliers, the expressions $\gamma_{\mu\nu}(\alpha_j, \alpha_k)$ $(\alpha_j \neq \alpha_k)$, $(\mu, \nu = 1, 2, 3, 4)$ are not all zero. Moreover as is well known the equation in the multipliers is not Abelian. But the group of a non-Abelian irreducible equation of degree three is of order six and permutes transitively the three pairs of roots. Hence, if $\gamma_{\mu\nu}(x, y)$ does not vanish for one pair of distinct roots, it does not vanish for any other pair. Now, there are three distinct quantities of type $(\alpha_j^m \alpha_h^n + \alpha_j^n \alpha_h^m)$ $(m, n = 0, 1, 2)$ between which there is no relation with integral coefficients. Hence (No. 96) $1 + k = 3 + 3 = 6 > 2p - 1$ and Ω if it exists at all is necessarily impure.

When Ω is pure the three multipliers must then be real. We know then that Ω always exists provided that the ratios τ_{j2}/τ_{j1} are not real. When they are arbitrary, we have $1 + h = 1 + k = 3$. The existence of a new alternate form either will bring us back to the case of No. 115 or else will make $1 + k$ take the value $6 > 2p - 1$, hence Ω will be impure. The same will hold for the non-alternate forms.

117. Let finally $r = 3$, $q = 2$. Since r is odd, the multipliers must be imaginary. The matrix Ω is isomorphic to a matrix composed with two arrays,

$$\tau \equiv \| \tau_{j1}, \tau_{j2}, \tau_{j3} \|, \qquad \| 1, \alpha_j \| \qquad (\alpha_1 = \alpha_2 = -\alpha_3 = i\sqrt{d}),$$

where d is again a positive integer and not a perfect square. The determinants of order two, derived from the first two rows of τ, cannot all be zero, for otherwise Ω would have two rows with proportional terms. Finally if $\tau_{31} = \tau_{32} = 0$, Ω contains an elliptic submatrix. Hence if Ω is pure, we can always replace τ by an array of the type

$$\left\| \begin{array}{lll} 1, & 0, & \tau_1 \\ 0, & 1, & \tau_2 \\ 1, & \tau_4, & \tau_3 \end{array} \right\| .$$

Since we have made no transformation upon the columns, we may take as form (19)

$$\gamma_{11}(\alpha_j, \bar{\alpha}_j) x_1 y_1 + \gamma_{22}(\alpha_j, \bar{\alpha}_j) x_2 y_2 + \gamma_{33}(\alpha_j, \bar{\alpha}_j) x_3 y_3 .$$

The numbers $\frac{-1}{2i} \gamma_{jj}(i\sqrt{d}, -i\sqrt{d}) = a_j$ are real numbers of the domain $K(i\sqrt{d})$—they are therefore rational numbers and we can without inconvenience assume that they are integers. In order that Ω be a Riemann matrix it is necessary (*a*) that $a_1 x_1 y_1 + a_2 x_2 y_2 + a_3 x_3 y_3$ vanish when the (x)'s are replaced by the elements of the first or second rows and the (y)'s by those of the third; (*b*) that $a_1 x_1 \bar{x}_1 + a_2 x_2 \bar{x}_2 + a_3 x_3 \bar{x}_3$ be positive at the point $(\lambda, \mu, \lambda\tau_1 + \mu\tau_2)$ whatever λ, μ, and negative at the point $(1, \tau_4, \tau_3)$.

We have, therefore, the relations

$$a_1 + a_3 \tau_1 \tau_3 = 0, \qquad a_2 \tau_4 + a_3 \tau_2 \tau_3 = 0,$$

then the inequalities

$$a_1 + a_2 \tau_4 \bar{\tau}_4 + a_3 \tau_3 \bar{\tau}_3 < 0$$

$$(a_1 + a_3 \tau_1 \bar{\tau}_1) \lambda\bar{\lambda} + a_3 \tau_1 \bar{\tau}_2 \lambda\bar{\mu} + a_3 \bar{\tau}_1 \tau_2 \bar{\lambda}\mu + (a_2 + a_3 \tau_2 \bar{\tau}_2) \mu\bar{\mu} > 0.$$

Hence the roots of the equation in ξ

$$\begin{vmatrix} a_1 + a_3 \tau_1 \bar{\tau}_1 - \xi, & a_3 \tau_1 \bar{\tau}_2 \\ a_3 \bar{\tau}_1 \tau_2, & a_2 + a_3 \tau_2 \bar{\tau}_2 - \xi \end{vmatrix} = 0$$

must both be positive. Moreover the coefficient of $\lambda\bar{\lambda}$ in the Hermitian form in λ, μ must be positive, which gives us finally the inequalities

$$\begin{aligned} &a_1 + a_3 \tau_1 \bar{\tau}_1 > 0, \\ &a_1 + a_2 + a_3 (\tau_1 \bar{\tau}_1 + \tau_2 \bar{\tau}_2) > 0, \\ &a_1 a_2 + a_3 (a_2 \tau_1 \bar{\tau}_1 + a_1 \tau_2 \bar{\tau}_2) > 0. \end{aligned}$$

Let us set

$$a_1 = -ma_3, \qquad a_2 = -na_3, \qquad \tau_j = R_j e^{i\phi_j}.$$

The array τ assumes then the form

$$\tau \equiv \begin{Vmatrix} 1, & 0, & m/\tau_3 \\ 0, & 1, & n\tau_4/\tau_3 \\ 1, & \tau_4, & \tau_3 \end{Vmatrix},$$

and our inequalities reduce to

$$\begin{aligned} &ma_3 (m - R_3^2) > 0, \\ &a_3 (m^2 + n^2 R_4^2 - (m + n) R_3^2) > 0, \\ &a_3 (m + nR_4^2 - R_3^2) > 0, \qquad mn < 0. \end{aligned}$$

Let us consider m, n as rectangular point coördinates and draw the curves representing the functions in the left-hand sides of these inequalities (ellipse with axes parallel to the coördinate axes and straight lines):
The point (m, n) can only be in one of the two regions, I, II, III. If it is in one of the first two regions, we must take $a_3 > 0$, and if it is in the third, we must take $a_3 < 0$. One of these regions always exists, hence τ_3, τ_4 can take arbitrary values, zero excepted. Under these conditions, we shall have $1 + k = 1$, $h = 2$, and the matrix is not singular—it is the simplest matrix of this type of genus $p > 1$.

If the matrix possesses a new non-degenerate bilinear form

$$\sum \gamma_{\mu\nu} (\alpha_j, \alpha_k) x_\mu y_\nu$$

it is impossible that $\gamma_{\mu\nu} = 0$ for $\alpha_j \neq \alpha_k$ if Ω is pure. Indeed then, if $\alpha_j = \alpha_k$, either the equation obtained, $\sum \gamma_{\mu\nu} (i\sqrt{d}, i\sqrt{d}) x_\mu y_\nu = 0 \quad (\alpha_k = \alpha_j)$,

represents a linear complex, necessarily degenerate since the containing space is of odd dimensionality, or else

$$\sum [\gamma_{\mu\nu}(i\sqrt{d}, i\sqrt{d}) + \gamma_{\nu\mu}(i\sqrt{d}, i\sqrt{d})] x_\mu x_\nu = 0 \qquad (\alpha_j = \alpha_k)$$

is a conic containing all the points of the line that joins $(1, 0, n/\tau_3)$ to $(0, 1, n\tau_4/\tau_3)$, conic necessarily degenerate. In all cases the reciprocity $\sum \gamma_{\mu\nu}(\alpha_j, \alpha_j) x_\mu y_\nu$ is degenerate and Ω is impure.

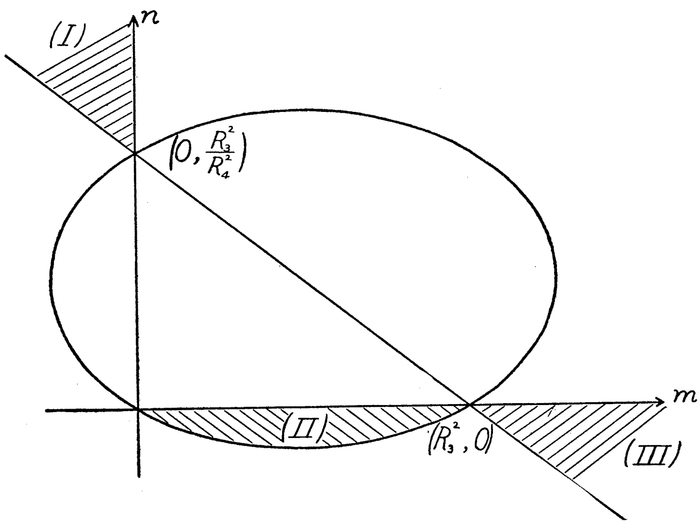

FIG. 1.

If the expressions $\gamma_{\mu\nu}(\alpha_j, \alpha_k)$ are not all zero, Ω will possess two reciprocities of the type

$$\sum \gamma_{\mu\nu}(\alpha_j, \alpha_k) x_\mu y_\nu = 0,$$

$$\gamma_{\mu\nu}(\alpha_j, \alpha_j) = 0; \qquad \gamma_{\mu\nu}(\alpha_j, \alpha_k) \neq 0 \text{ if } \alpha_j \neq \alpha_k.$$

If Ω is pure they are not degenerate and multiplying one of them by the inverse of the other we obtain then a new multiplication permutable with the one whose multipliers are the (α)'s. In that case Ω must possess a Riemann projectivity of degree $\geqq 2q$, hence of degree 6, and we fall back on the type of No. 115.

Thus for a pure matrix of genus three the only possible combinations for the invariants h, k are $(0, 0)$, $(0, 1)$, $(1, 1)$, $(2, 5)$. The corresponding matrices depend upon $6, 2, 3, 0$ essential parameters.

Chapter III. Abelian varieties with cyclic groups and varieties of rank > 1 images of their involutions

§ 1. Varieties of rank one with cyclic group

118. The study of hyperelliptic surfaces with cyclic group and more generally with finite group of birational transformations has already been made by Enriques, Severi, Bagnera and de Franchis. We only propose here to give a few new properties and to calculate the invariants of some simple varieties of genus $p > 2$ and rank > 1.

Every birational transformation of finite order T of an Abelian variety of rank one, V_p, whose Riemann matrix has been put in a suitable form, will be given by equations such as

$$(1)\qquad \begin{aligned} u_i' &= u_i + \alpha_i && (i = 1, 2, \cdots, p');\\ u_{p'+j} &= \epsilon_j\, u_{p'+j} + \alpha_{p'+j} && (j = 1, 2, \cdots, p - p'), \end{aligned}$$

where the (ϵ)'s are roots of unity other than one. A very interesting case and one to which we shall largely limit the discussion is that where the equations of T are

$$(2)\qquad u_j' = \epsilon^{n_j} u_j \qquad (j = 1, 2, \cdots, p),$$

the (ϵ^n)'s being primitive roots of a binomial equation $x^m = 1$. It will be particularly the case if Ω is pure. We shall assume $m > 2$. The numbers $\pm n_j$ will form a complete set of residues prime to m taken r times so that if $2\mu = \varphi(m)$, where φ is the Euler function, then $r = p/\mu$.

We have shown how we may derive from Ω a matrix Ω' composed with two arrays

$$\tau \equiv \| \tau_{j1}, \tau_{j2}, \cdots, \tau_{jr} \|, \qquad \| 1, \epsilon^{n_j}, \cdots, \epsilon^{(2\mu-1)n_j} \| \qquad (j = 1, 2, \cdots, p).$$

To this matrix corresponds an Abelian variety of rank one, V_p', in correspondence $(n, 1)$ with V_p if the array τ is suitably chosen. V_p' is the image of an ordinary involution of order n on V_p and possesses a cyclic birational transformation expressed by the same equations (2). Now it is easy to show that from the point of view which will occupy us, we may replace V_p by V_p', that is, Ω by Ω', and this we propose to do in the sequence. We shall then assume that Ω coincides with Ω'.

When τ is as general as possible and the (ϵ^n)'s are not all different, the invariants of V_p are given by $1 + h = 2(1 + k) = 2\mu$, while if these multipliers are different $(r = 2)$, they are given by $1 + h = 4\mu$, $1 + k = 3\mu$.

119. The determination of the total group of birational transformations of a V_p is of considerable interest. For $p = 2$, this has already been done by Scorza in his *Palermo Rendiconti* memoir. We shall show how the solution of this question is related in an important case to the problem of the determination of the units of an algebraic domain.

Let G be a permutable subgroup of the group formed by the products of the complex multiplications, such that no Riemann projectivity corresponding to one of its operations transforms separately a submatrix of Ω if Ω is impure. We shall endeavor to characterize the operations of G which lead to birational transformations of V_p.

Let T be a birational transformation belonging to G and

$$B \equiv \| b_{\nu\mu} \| \qquad (\nu, \mu = 1, 2, \cdots, 2p)$$

its Riemann projectivity. We know that the determinant $|b_{\nu\mu}| = \pm 1$. Moreover there exists a minimum base $B_1, B_2, \cdots, B_q$ for the projectivities whose terms are integers and we have $B = \sum \lambda_j B_j$, where the (λ)'s are integers. If $\alpha_1^j, \alpha_2^j, \cdots, \alpha_p^j$ are the multipliers of B_j we have for those of B

$$\alpha_s = \sum_j \lambda_j \alpha_s^j \qquad (s = 1, 2, \cdots, p)$$

and their norm is equal to unity. They are therefore conjugate units of a certain algebraic domain, and more especially α_s is a unit contained in the modulus $(\alpha_1^s, \alpha_2^s, \cdots, \alpha_q^s)$. We may remark in passing that each number of this modulus determines a Riemann projectivity whose terms are integers. Moreover the modulus is an *order* in the sense of Dedekind. For, if α_s' and α_s'' belong to it, there correspond to them projectivities with integral terms B', B'', and $\alpha_s' \alpha_s''$ which is multiplier of the projectivity with integral terms $B'B''$ belongs actually to the same modulus. Thus α_s is a unit contained in a certain order of algebraic numbers and conversely if α_s is such a unit, it defines a projectivity with integral terms whose determinant is unity, hence a birational transformation of V_p. Thus the projectivities corresponding to the birational transformations, *and therefore the birational transformations themselves, are combined like units in an order of an algebraic domain.* From a classical theorem due to Dirichlet, follows then that there exists a finite number of permutable birational transformations $T_1, T_2, \cdots, T_\nu$, $\nu < p/r$, such that any other is given by a relation

$$T = T_0 T_1^{n_1} T_2^{n_2} \cdots T_\nu^{n_\nu},$$

where T_0 is an arbitrary cyclic transformation of the system and ν is the number of distinct real multipliers increased by half the number of imaginary multipliers.

Let $\beta_1^j, \beta_2^j, \cdots, \beta_s^j$ be a minimum base for the integers of the domain $K(\alpha_j)$. The solution of the problem which we are considering is related to that of the following: To solve in integers x_j the equation

$$\prod_j \sum_k \beta_k^j x_k = \pm 1.$$

We see that the group of birational transformations of G, like G itself, depends

solely upon the equation $f(\alpha) = 0$ but not upon the array τ provided that $r \neq 2$.

In the particularly interesting case where the roots of $f(\alpha) = 0$ are all imaginary, each being given by the same rational function of its conjugate, the problem is somewhat simplified. Let us set $\alpha_j + \bar{\alpha}_j = 2\zeta_j$, $\alpha_j \bar{\alpha}_j = \eta_j$, and assume the multipliers so chosen that the (ζ)'s are all distinct. The norm of η_j is obviously *one* and the problem is therefore reduced to finding the real units of the real domain $K(\zeta_j)$ defined by an irreducible equation of degree p/r, $\phi(\zeta) = 0$, (No. 89).

Remarks: (I) There exist no cyclic birational transformations permutable with a given transformation T of order q^m, (q prime), other than the powers of T itself. This follows from the fact that if $\epsilon = e^{2\pi i/q^m}$, the algebraic domain $K(\epsilon)$ contains no other roots of unity than the powers of ϵ.

(II) With T still of order q^m, (q prime), and if $r > 1$, we may apply certain considerations of No. 90. If the numbers ϵ^{n_j} are invariant under a subgroup of order n of the equation in the q^m-th primitive roots of unity, the period matrix is composed with n submatrices of genus $p' = p/n$. If there exists a complex multiplication with multipliers of degree $> n$, the corresponding irreducible equation must be reducible in the domain $K(\epsilon)$. But according to a well-known theorem on the cyclic units of a cyclic domain of degree q^m, if these multipliers are roots of unity they must be themselves powers of q. It follows that if the order ν of a birational transformation is such that $\varphi(\nu) > n$, then $\nu = q^a \leqq q^m$. In particular, if $m = 1$, then $\nu = q$.

120. As an application, we shall establish, in a different manner, the results obtained by Scorza on the birational transformations of pure hyperelliptic surfaces when the multipliers are roots of an irreducible equation of degree four. Let $u_1' = \alpha_1 u_1$, $u_2' = \alpha_2 u_2$ be the equations of the birational transformation. The expressions $\alpha_1 + \bar{\alpha}_1$ and $\alpha_1 \bar{\alpha}_1$ are integers of a quadratic domain $K(\sqrt{d})$ where d is a positive integer, not a perfect square, and $\alpha_1 \bar{\alpha}_1$ is a unit of this domain. Hence α_1 satisfies an equation

$$\alpha^2 + (m + n\sqrt{d})\alpha + t + u\sqrt{d} = 0,$$

where m, n, t, u are integers or halves of integers and $t^2 - du^2 = \pm 1$. The number α_2 satisfies the equation obtained when $\sqrt{d}$ is replaced by $-\sqrt{d}$.

In order that these two numbers be imaginary, it is necessary that

$$(m + n\sqrt{d})^2 < 4(t + u\sqrt{d}), \qquad (m - n\sqrt{d})^2 < 4(t - u\sqrt{d}).$$

Hence $(m^2 - dn^2)^2 < 16$, and therefore $|\text{norm}\,(m + n\sqrt{d})| = |\beta| = 1, 2,$ or 3. The surface possesses the birational transformations whose multipliers are α_1^n, α_2^n, n being an arbitrary integer. Hence, also $|\text{norm}\,(\alpha_1^n + \bar{\alpha}_1^n)| = 1,$

2, or 3. Now if we set

$$(m + n\sqrt{d})^2(t - u\sqrt{d}) = \xi + \eta\sqrt{d},$$

and observe that $\xi^2 - d\eta^2 = \beta^2$, we obtain by an easy computation

$$\text{norm}\,(\alpha_1^3 + \overline{\alpha}_1^3) = \beta(\beta^2 - 6\xi + 9) = \beta',$$
$$\text{norm}\,(\alpha_1^4 + \overline{\alpha}_1^4) = (\beta^2 - 4\xi + 4)^2 - 4(2\xi^2 - \beta^2 - 4\xi + 4) = \beta''.$$

Hence if $\beta = \pm 3$ we must also have $\beta' = \pm 3$, $18 - 6\xi = \pm 1$, which is impossible since 2ξ is an integer. Similarly, if $\beta = \pm 2$, $\beta' = \pm 2$ and $13 - 6\xi = \pm 1$, which requires that $\beta' = \beta$, $\xi = 2$. But in that case $\beta'' = 0$, which is impossible since d is not a perfect square. It follows necessarily that $\beta = \pm 1$. We conclude from this that

$$(5 - 4\xi)^2 - 4(2\xi^2 - 4\xi + 3) = \beta'',$$

or

$$\xi^2 - 3\xi + \tfrac{1}{8}(17 - \beta'') = 0,$$

whence

$$\xi = \frac{1}{2}\left[3 \pm \sqrt{9 - \frac{17 - \beta''}{2}}\right].$$

For $\beta'' = 1$, we obtain $\xi = 1$ or 2. But for $\xi = 1$, $\beta' = \pm 4$, and for $\xi = 2$, $\beta' = \pm 2$. Hence $\beta'' = -1$, $\xi = 3/2$, and therefore $d = \dfrac{\xi^2 - 1}{\eta^2} = \dfrac{5}{(2\eta)^2}$, and finally $\eta = \pm\frac{1}{2}$, $d = 5$. Ultimately, then, we obtain

$$(m + n\sqrt{5})^2 = (t + u\sqrt{5})\left(\frac{3 \pm \sqrt{5}}{2}\right),$$
$$t + u\sqrt{5} = (m + n\sqrt{5})^2\left(\frac{3 \pm \sqrt{5}}{2}\right).$$

The quantity $\delta = \frac{1}{2}(1 + \sqrt{5})$ is the fundamental unit of the domain $K(\sqrt{5})$. Hence

$$m + n\sqrt{5} = \delta^\nu, \qquad t + u\sqrt{d} = \delta^{2(\nu \pm 1)},$$

and therefore α satisfies one of the two equations

$$\alpha^2 + \delta^\nu\alpha + \delta^{2(\nu\pm 1)} = 0.$$

If we observe that for $\nu = 1$ the second has for root $\epsilon = e^{2\pi i/5}$, we find for ζ, if we set $\mu = \nu - 1$, the two values $\epsilon\delta^\mu$, $(\epsilon + \epsilon^{-1})^\mu\left(\dfrac{2\epsilon - 1 + \delta}{2}\right)$, or else, since $\delta = \epsilon + \epsilon^{-1}$, the values

$$\epsilon(\epsilon + \epsilon^{-1})^\mu, \qquad (\epsilon + \epsilon^{-1})^\mu\left(\frac{3\epsilon + \epsilon^{-1} - 1}{2}\right).$$

Having taken for α_1 one of these values we obtain α_2 by replacing everywhere

ϵ by ϵ^2 or ϵ^3. The corresponding matrices are isomorphic to

$$\begin{Vmatrix} 1, & \alpha_1, & \alpha_1^2, & \alpha_1^3 \\ 1, & \alpha_2, & \alpha_2^2, & \alpha_2^3 \end{Vmatrix}.$$

For $\mu = 0$ and α of the first type, we have the matrix

$$\begin{Vmatrix} 1, & \epsilon, & \epsilon^2, & \epsilon^3 \\ 1, & \epsilon^2, & \epsilon^4, & \epsilon \end{Vmatrix}$$

to which they are all isomorphic and it corresponds to the surface of Jacobi-Humbert investigated by Scorza or the Jacobi surface of the curve

$$y^2 = x(x^5 + 1),$$

which possesses a cyclic transformation of order 5.

Remark: We have assumed everywhere that d is not a perfect square. In the contrary case $t + u\sqrt{d} = \pm 1$, $m + n\sqrt{d} = \mu$, integer, and α_1 is a root of $\alpha^2 + \mu\alpha \pm 1 = 0$. The surface possesses then a birational transformation with multipliers of degree two.

§ 2. Multiple points of abelian varieties of rank > 1

121. Let us designate by W_p the Abelian variety of rank m, image of the cyclic involution (1) or (2). The multiple points of W_p are images of the coincidence points of the involution on V_p. If the transformation T corresponds to the equations (1) we shall obtain the coincidence points if we obtain the solutions of the following equations in the unknown integers x_μ,

$$u_i + \sum_{\mu=1}^{2p} x_\mu \omega_{i\mu} = u_i + \alpha_i \qquad (i = 1, 2, \cdots, p');$$

$$u_{p'+j} + \sum_{\mu=1}^{2p} x_\mu \omega_{p'+j,\mu} = \epsilon_j u_{p'+j} + \alpha_{p'+j} \qquad (j = 1, 2, \cdots, p - p').$$

If $p' < p$, there is no solution when the (α)'s of index $i \leqq p'$ are not all zero and there is an infinity of them when they all are. In this last case the problem is reduced to the determination of the coincidence points of an involution on a $V_{p-p'}$. Let us assume then that $p' = 0$, or that the equations of T are of the form

$$u_i' = \epsilon_i u_i + \alpha_i \qquad (i = 1, 2, \cdots, p).$$

The coincidence points are all given by the formula

$$u_i = \frac{-\alpha_i}{\epsilon_i - 1} + \sum_{\mu=1}^{2p} \frac{x_\mu \omega_{i\mu}}{\epsilon_i - 1} \qquad (i = 1, 2, \cdots, p).$$

Let $(x_1^0, x_2^0, \cdots, x_{2p}^0)$ be a solution in integers. If we add to the (x^0)'s a solution of the system

$$\sum_{\mu=1}^{2p} \frac{x_\mu \omega_{i\mu}}{\epsilon_i - 1} = \sum_{\mu=1}^{2p} y_\mu \omega_{i\mu} \qquad (i = 1, 2, \cdots, p),$$

the (y)'s being also integers, we shall always obtain the same coincidence point. Now, let

$$\epsilon_i \, \omega_{i\mu} = \sum_{\nu=1}^{2p} a_{\nu\mu} \, \omega_{i\nu} \qquad (i = 1, 2, \cdots, p; \mu = 1, 2, \cdots, 2p),$$

be the Riemann projectivity belonging to T. The above system can be written

$$\sum_{\mu=1}^{2p} x_\mu \, \omega_{i\mu} = - \sum_{\mu=1}^{2p} y_\mu \, \omega_{i\mu} + \sum_{\mu, \nu}^{1 \cdots 2p} y_\mu \, a_{\nu\mu} \, \omega_{i\nu} \qquad (i = 1, 2, \cdots, p),$$

and therefore

$$x_\mu = - y_\mu + \sum_{\nu=1}^{2p} a_{\mu\nu} \, y_\nu \qquad (\mu = 1, 2, \cdots, 2p).$$

Let us set

$$a_{\mu\mu} - 1 = b_{\mu\mu}, \qquad a_{\mu\nu} = b_{\mu\nu} \qquad \text{if} \qquad \mu \neq \nu,$$

and let $B_{\mu\nu}$ be the coefficient of $b_{\mu\nu}$ in the expansion of the determinant

$$B = |b_{\mu\nu}| \qquad (\mu, \nu = 1, 2, \cdots, 2p),$$

whose value is

$$B = \prod_{i=1}^{p} (\epsilon_i - 1)(\epsilon_i^{-1} - 1) > 0.$$

The (x)'s satisfy the congruences

$$\sum_{\mu=1}^{2p} B_{\mu\nu} \, x_\nu \equiv 0, \text{ mod. } B \qquad (\nu = 1, 2, \cdots, 2p)$$

which possess B^{2p-1} distinct solutions in numbers included between zero and B.* Thus to each of the B^{2p} sets of values of the (x)'s all included between zero and B—and it is not necessary to consider any others—will correspond B^{2p-1} others giving the same coincidence point of the involution, hence the same multiple point of W_p. Therefore the number of these multiple points is precisely equal to B.

The value of B is easy to compute. Let $F(\alpha) = 0$ be the characteristic equation of the complex multiplication belonging to T. We have obviously $B = F(1)$. For the Kummer surface $F(\alpha) = (\alpha + 1)^4$, $B = 16$. For the hyperelliptic surface of rank 3 belonging to the matrix

$$\left\| \begin{matrix} 1, & \epsilon, & \tau, & \epsilon\tau \\ 1, & \epsilon^2, & \tau', & \epsilon^2 \tau' \end{matrix} \right\|, \qquad \epsilon = e^{2\pi i/3},$$

$F(\alpha) = (1 + \alpha + \alpha^2)^2$, $F(1) = 3^2 = 9$, which is actually the number found by Bagnera, de Franchis, Enriques, and Severi.

122. When m is arbitrary, the singular points are of different nature according as the corresponding points of V_p are coincidence points for all the powers

* Krazer, *Lehrbuch der Theta Functionen*, p. 57.

of T or for some of them only. We shall examine in detail the case of $m = q$, prime. The case of m arbitrary can be treated in very much the same way. We may also take the numbers α_i all equal to zero and we then have for the equations of T $u'_i = \epsilon^{n_i} u_i \quad (i = 1, 2, \cdots, p)$, where the numbers $\pm n_i$ form $2p/(q-1)$ times a complete set of residues modulo q. The neighborhoods of the multiple points are transitively permuted by a finite group of birational transformations of W_p which corresponds to a group of ordinary transformations of V_p (Bagnera and de Franchis). Hence the neighborhood of any one of them is equivalent to the same number κ of infinitesimal hyper-surfaces and, from the point of view of Analysis Situs, they behave alike. It is therefore sufficient to consider the multiple point corresponding to the coincidence point $u_1 = u_2 = \cdots = u_p = 0$.

The groups of points of the involution in the neighborhood of this coincidence point are in one-to-one correspondence with the groups of points of the involutions determined in an S_p by the homogeneous transformation of coördinates

$$\zeta x'_i = \epsilon^{n_i} x_i, \qquad \zeta x'_{p+1} = x_{p+1} \qquad (i = 1, 2, \cdots, p)$$

in the neighborhood of the coincidence point $O\ (0, 0, \cdots, 0, 1)$. Designate by M_p the image of this involution of S_p and by s the number of distinct exponents modulo q among the (n)'s. In the neighborhood of the multiple point O' of M_p transformed of O, there will be s distinct branches corresponding to the s infinitesimal varieties of coincidence of the involution in the neighborhood of O. Let us apply a quadratic birational transformation to the space containing M_p transforming it into a variety M'_p, this in such a manner that O' becomes a hyperplane H. The s branches just mentioned become, as far as their parts in the neighborhood of O' are concerned, the neighborhoods of s linear spaces of H, of which we shall designate any one by K''. To K'' corresponds on M_p an infinitesimal variety K' very near O', and on V_p an infinitesimal variety of coincidence K very near O. The $p-1$ dimensional elements of V_p passing through K undergo an involution whose representative equations with suitably chosen homogeneous parameters x_i are of the type

$$\begin{aligned} \zeta x'_i &= \epsilon^{n_i - n_h} \cdot x_i && (i = 1, 2, \cdots, t') \\ \zeta x'_{t'+l} &= x_{t'+l} && (l = 1, 2, \cdots, t\ ), \end{aligned}$$

where n_h is one of the indices n, perfectly defined when K is known. This involution is of the same type as previously except that we have now only $s-1$ distinct groups of exponents. In the neighborhood of K'' there will then be $(s-1)$ distinct branches of M'_p. This reasoning may be continued until we isolate elements in the vicinity of which there is only one branch. We shall then have $\kappa = s!$ In particular, if the (n)'s form a complete system of residues, then $\kappa = (q-1)!$ The singular points are therefore equivalent to

$B\kappa = Bs!$ infinitesimal algebraic hypersurfaces and therefore $\rho = [\rho] + Bs!$ We recall that when any invariant is written within square brackets, its value is assumed taken disregarding infinitesimal cycles (See No. 11).

Remark: The preceding discussion, followed by a reasoning analogous to that in No. 51, may lead to a proof that W_p is birationally transformable into a non-singular variety contained in a suitable space.

§ 3. Indices of connectivity of varieties of rank > 1

123. Let us assume the birational transformation of type (2). The matrix Ω is then equivalent to the matrix Ω' of No. 118. Designate by δ_h^μ the linear cycle of V_p corresponding to the period $\epsilon^{nh}\tau_{j\mu}$, by $(\delta_{h_1}^{\mu_1}, \delta_{h_2}^{\mu_2}, \cdots, \delta_{h_s}^{\mu_s})$ the s-cycle corresponding to the linear cycles in parenthesis, and by $(\bar\delta_{h_1}^{\mu_1}, \bar\delta_{h_2}^{\mu_2}, \cdots, \bar\delta_{h_s}^{\mu_s})$ the corresponding cycle on W_p. On this last variety

$$(\bar\delta_{h_1}^{\mu_1}, \cdots, \bar\delta_{h_s}^{\mu_s}) \sim (-1)^n(\bar\delta_{k_1}^{\nu_1}, \cdots, \bar\delta_{k_s}^{\nu_s})$$

if the sets of integers (μ), (ν) differ only by their order and if moreover, when $\mu_d = \nu_{d'}$, then $h_d = k_{d'} + \nu$. The integer n indicates the number of inversions when we pass from one of the systems of superscripts to the other. The cycles $(\bar\delta_{h_1}^{\mu_1}, \bar\delta_{h_2}^{\mu_2}, \cdots, \bar\delta_{h_s}^{\mu_s})$ form therefore a base for the finite cycles on W_p. It is not in general possible to give an exact formula for $[R_s]$, but we can give a geometrical process to obtain this number. Let first $p = \mu$, $s = 2$. We mark on a circle the vertices $1, 2, \cdots, m$ of a regular m-sided polygon and denote by $r_1, r_2, \cdots, r_{2\mu}$ the numbers which are prime to m and $< m$. We join the vertices r_i to each other and the number of segments of distinct length thus obtained is equal to $[R_2]$. Similarly $[R_s]$ is the number of distinct incongruent convex polygons having for vertices s of the points r_i. If $p > \mu$, $r > 1$, we take rn division points and use the points r_i, $r_i + m, \cdots$, $r_i + (r-1)m$ as the vertices of convex polygons.

124. *Case of $m = q$, odd prime.* We can then obtain simple formulas for the indices. Let first $2p = q - 1$. An s-sided convex polygon will be determined by s integers whose sum is q, say $h_1, h_2, \cdots, h_s$. Two convex polygons that correspond to partitions $h_1, h_2, \cdots, h_s$, and $h_1', h_2', \cdots, h_s'$, of q will be congruent if $h_i' - h_i = h_k' - h_k$ $(i, k = 1, 2, \cdots, s)$. But in all there are $\binom{q-1}{s-1}$ arrangements of s integers yielding a sum q. Taking account of the possibility of permuting cyclically the (h)'s, we obtain $[R_s] = \frac{1}{s}\binom{2p}{s-1}$. This number is actually an integer for $\binom{q}{s} = \frac{q}{s}\binom{q-1}{s-1}$ is an integer and s is prime to q. In particular $[R_2] = p$. We can similarly obtain $[R_s]$ whatever r, but we will merely indicate here the formula, easy to obtain, $[R_2] = \frac{1}{2}r^2(q-1)$.

125. *Formula for R_2.* If we assume that the infinitesimal algebraic cycles in the vicinity of the multiple points are all independent, we have $R_2 = [R_2] + B\kappa$. To prove that this is actually the case, it is sufficient to show that the infini-

tesimal hypersurfaces in the neighborhood of these points are algebraically distinct. We shall merely give some rapid indications on this question:— A, B being any two of them we take suitable multiples C, D of the hyperplane sections passing the one through A and the other through B, then two hypersurfaces, C_1, D_1, of the same systems infinitely near C, D respectively, but passing through neither A nor B. We have $[C^i D^{p-i}] = [C_1^i D_1^{p-i}]$, $i > 0$, hence at once $[A^i B^{p-i}] = 0$. By considering then two hypersurfaces through A, it may be shown that $[A^p] \neq 0$. Finally $[A^i H^{p-i}] = 0$, $p > i > 0$, for every H of W_p not passing through the multiple points. By a reasoning of Severi's follows readily that the infinitesimal hypersurfaces of W_p are algebraically distinct. Moreover, if $H_1, H_2, \cdots, H_{[\rho]}$ form a base for the hypersurfaces of W_p when we neglect the multiple points, there is no relation between the (H)'s and the infinitesimal hypersurfaces. These facts have been established by other methods for the case $p = 2$ by Severi, Bagnera, and de Franchis.

126. Let us pass now to the determination of the invariants $[\sigma_s]$, σ_s, σ. Let Δ be a non-zero s-cycle of V_p such that no sum of less than m of the cycles $T^k \Delta$ be ~ 0 but $\sum_0^{m-1} T^k \Delta \sim 0$. If Δ_1 is a cycle which is not homologous to the cycles $T^k \Delta_1$ $(0 < k < m)$, we can take $\Delta = T\Delta_1 - \Delta_1$. Let δ be the cycle corresponding to Δ on W_p. If $k\delta$ bounds on W_p, $\Delta + T\Delta + \cdots + T^{k-1} \Delta$ must bound on V_p. Hence according to the assumption made, we must have $k = m$. Moreover, we have actually $m\delta \sim 0$ and therefore *δ is a zero divisor for the s-cycles of W_p.* Are we really dealing with actual zero divisors? This is certainly the case if W_p is without multiple points, that is, if there are no coincidence points on V_p. Then, if $m = q$, prime, σ_s is of the form m^a and in particular $\sigma = \sigma_1 = q^r$; $r = 2p'/(q-1)$, $p - p'$ being the genus of the submatrix maintained invariant by T.

Let us return now to the case where there is a finite number of coincidence points. I say that then $\sigma_1 = \sigma_{2p-2} = \sigma = 1$. For, if A is a finite hypersurface of V_p, algebraically distinct from its transformed by the powers of T, B a variable hypersurface of the same continuous system as A, while A', B' are the corresponding hypersurfaces of W_p, then $A' - B'$ is to be considered as a divisor of zero and we obtain all those divisors in this manner since they are all algebraic. Now, let B approach a coincidence point. B' will approach a singular point, and at the limit $A' - B'$ will have become a zero divisor *if we consider the singular points as ordinary points,* but certainly not if we bring into play the infinitesimal hypersurfaces in the neighborhood of the singular point, for then $A' - B'$ will be equal to a sum of such hypersurfaces. Hence on the variety with ordinary singularities birationally equivalent to W_p, $A' - B'$ will not be a zero divisor and we shall have $\sigma = 1$. This is in agreement with the results of Severi, Bagnera, and de Franchis.

§ 4. Integrals of the first kinds. Invariants ρ, $[\rho]$, ρ_s

127. When W_p is the image of an involution generated by a transformation (1), it possesses p' simple integrals of the first kind, hence if $p' = 0$, W_p is regular.

Let us assume then W_p regular. When we express the coördinates in terms of the (u)'s, a k-uple integral of the first kind must assume the form

$$\sum A_{j_1 j_2 \cdots j_k} \int\int \cdots \int du_{j_1}\, du_{j_2} \cdots du_{j_k},$$

and remain invariant when we apply T. We may assume T in the form (2) since the (α)'s have nothing to do with the question. We must then have $n_{j_1} + n_{j_2} + \cdots + n_{j_k} \equiv 0$, mod. m, unless $A_{j_1 j_2 \cdots j_k} = 0$. Thus, every integral of the first kind is a linear combination of the integrals invariant under T. The converse proposition is obvious.

I say now that *if T is of the form* (2), *does not maintain invariant any reducible system of integrals of the first kind, and maintains invariant a k-uple integral of the first kind* $(k > 1)$, *then W_p does not contain any congruence of spaces.**

By *congruence* we mean a system of algebraic manifolds such that one and only one passes through a given point of W_p. For there will be an invariant integral such as $\int\int \cdots \int du_1\, du_2 \cdots du_k$. The variety W_p contains a ruled k-dimensional variety M'_k, locus of straight lines of which one goes through every point of the variety. Such a variety possesses no k-uple integrals of the first kind—this can be proved as done by Picard for $k = 2$. Hence on M'_k the above integral reduces to a constant. It follows that on M'_k, and therefore on the corresponding variety M_k of V_p, several of the differentials du, for example $du_1, du_2, \cdots, du_l$, vanish, and hence at once that $u_1, u_2, \cdots, u_l$ form a system of reducible integrals invariant by T.† This contradiction proves our theorem.

128. When Ω is of the type of No. 118 with $r > 1$ and T does not transform into itself any system of reducible integrals, there will certainly be invariant integrals. For the (n)'s are certainly not composed with r times the same set of μ exponents. There will then certainly be two whose sum is m and therefore at least one double integral will be invariant. In particular, *if Ω is pure and $r \geqq 2$, W_p does not possess any congruence of spaces.*

129. Let us show that *what we have just stated still holds if $r = 1$ and m is a prime number, $q > 7$.* For since the characteristic equation corresponding to T is irreducible there will then be no system of reducible integrals invariant by T. Everything reduces therefore to establishing that among the (n)'s we can always find a set $n_1, n_2, \cdots, n_k$ whose sum is divisible by q. The

* For $p = 2$ this has been proved by Enriques and Severi.

† *Castelnuovo*, Rendiconti dei Lincei (1905).

condition $k > 2$ must be added as follows from the fact that none of the (n)'s may be conjugate to each other.

If $p < n_j < 2p+1 = q$, we can replace n_j by $-q+n_j$. Hence, modulo q, $n_1, n_2, \cdots, n_p$ are nothing more nor less than the numbers $1, 2, \cdots, p$ affected with an arbitrary combination of signs and we have to prove the following: Whatever these signs, we can always form, with some of the numbers of the set, a sum divisible by q.

Now, we may at once verify the following: If the integers $1, 2, 3, 4, 5$ are not all affected with the same sign, we may form with them a zero sum except when 1 or 2 are taken with one sign and the four others with the opposite sign. In these two cases, it is easy to verify that we may form a sum equal to ± 11. Hence the theorem is true for $q = 11$. Assume $q > 11$. We can change all the signs, hence we may assume 3 taken positively. Let then α be the first integer > 5 taken negatively. If $\alpha = 6$, we have the following three possibilities as to the signs of the first six integers and for which there may be doubt:

$$1, 2, 3, 4, 5, -6; \qquad -1, 2, 3, 4, 5, -6; \qquad 1, -2, 3, 4, 5, -6.$$

In the first two cases $2+4-6=0$ and in the third $-2+3+5-6=0$. If $\alpha > 6$ and α is even, in the only doubtful case where $3, 4, 5$ are all taken with the same sign $+$, the combination $\frac{1}{2}\alpha - 1$, $\frac{1}{2}\alpha + 1$, $-\alpha$ gives a zero sum, while if α is odd, the combination $\frac{1}{2}(\alpha+1)$, $\frac{1}{2}(\alpha-1)$, $-\alpha$ yields the same result. The theorem is therefore proved.

130. *Numbers* ρ, $[\rho]$, ρ_0. Let us take again for matrix Ω the matrix of No. 118. In the notations used above $[\rho]$ is the number of algebraic cycles of V_p of type

$$\sum_{\mu, \nu, s} a_{\lambda, \nu, s} \sum_{t=1}^{2\mu} (\delta_\lambda^t, \delta_\nu^{s+t}).$$

The period of $\int\int du_j\, du_k$ with respect to this cycle is

$$\sum a_{\lambda, \nu, s} \sum_t \left(\tau_{j\lambda}\tau_{k\nu}\epsilon^{n_j(t-1)+n_k(s+t-1)} - \tau_{j\nu}\tau_{k\lambda}\epsilon^{n_j(s+t-1)+n_k(t-1)}\right),$$

and it is zero as we might expect when $n_j + n_k \not\equiv 0$, mod. m, whereas for $n_j \equiv -n_k$, mod. m, it has the form

$$\sum \gamma_{\lambda\nu}(\epsilon^{n_j}, \epsilon^{-n_j})\tau_{j\lambda}\tau_{k\nu} \qquad (\gamma_{\lambda\nu}(x, y) = -\gamma_{\nu\lambda}(y, x)),$$

where $\gamma_{\lambda\nu}$ is a polynomial with integral coefficients. Hence $[\rho] = (1 + k_0)$ where k_0' is the number defined in No. 107. As to the other invariants, we have

$$\rho_0 = [R_2] - [\rho], \qquad \rho = [\rho] + B\cdot\kappa.$$

In particular, if $m = q$, prime, and if τ is general, then $[\rho] = 1$,

$\rho_0 = \frac{1}{2}r^2(q-1) - 1$. If $r = 1$, we never have $n_j + n_k \equiv 0$, mod. m, all the periods of the nature in question are zero, hence $[\rho] = [R_2]$, $\rho_0 = 0$. Thus the variety of rank m corresponding to the matrix

$$\| 1, \epsilon^{n_j}, \cdots, \epsilon^{(2p-1)n_j} \| \qquad (j = 1, 2, \cdots, p)$$

has neither double integrals of the first kind nor double integrals of the second kind.

Chapter IV. A class of algebraic curves with cyclic group and their Jacobi varieties

§ 1. Integrals of the first kind of the curve $y^q = \prod_i (x - a_i)^{\alpha_i}$ (q odd prime)

131. The object of this chapter is the investigation of the curves

$$(1) \qquad y^q = \prod_{i=1}^{r+2} (x - a_i)^{\alpha_i} \qquad (q \text{ odd prime})$$

characterized by the possession of a cyclic group of genus zero. Their importance consists in that their Jacobi varieties are the most interesting example of the varieties discussed in Chapter II. Furthermore they belong to a class much studied by various authors especially in regard to the presence of reducible systems of integrals of the first kind. We believe that the results here given constitute the most far-reaching investigation along that line. The restriction of q to odd primes is of course narrowing, yet it is amply compensated by the greater elegance of the results obtained. Very likely much of the discussion that follows holds for any q, and perhaps even when the group is of genus other than zero.

132. Let p be the genus of (1) which we shall call C_p in the sequence, and T the cyclic transformation,

$$x = x', \qquad y = \epsilon y'; \qquad \epsilon = e^{\frac{2\pi i}{q}}.$$

T leaves no rational point function on C_p invariant other than those rational in x alone. $R(x)$ being such a function, any other can be expressed as a rational function of $R(x)$, if and only if x itself can be, which requires that $R(x) = (ax + b)/(cx + d)$. Hence x is characterized by being invariant under T, and, up to a projective transformation, by the fact that any other point function on C_p invariant under T is rational in x. Thus x is determined by properties invariant under any birational transformation. The anharmonic ratios of the values of x at the critical points, or coincidence points of T, are therefore invariant relatively to birational transformations, and as they completely determine C_p those which are functionally independent among them can be taken as the independent moduli of the curve.

The point $A_i(a_i, 0)$ is *critical* for the function $y(x)$ if α_i is not divisible by q. If $r' + 2$ is the number of critical points, *C_p depends upon $r' - 1$ moduli.*

Let C_p' be a curve

$$y^q = \prod_i (x - a_i')^{\alpha_i'}$$

birationally equivalent to C_p and this in such a manner that T becomes a transformation of similar form say

$$x = x', \qquad y = \epsilon^k y'$$

for C_p'. Let

$$x' = R_1(x, y), \qquad y' = R_2(x, y)$$

be the transformation changing C_p into C_p'. Since R_1 and R_2^q are invariant under T, R_1 must be rational in x, and as x must be rational in R_1 we have $R_1(x) = (ax + b)/(cx + d)$. The conditions relatively to

$$R_2(x, y) = R_2(x, \prod_i (x - a_i)^{\frac{\alpha_i}{q}})$$

require that R_2 be of the form $y^n \cdot R(x)$, where n is an integer prime to q. Hence the transformation from C_p to C_p' must be of the form

$$x' = \frac{ax + b}{cx + d}, \qquad y' = y^n \cdot R(x). \tag{2}$$

Conversely if C_p can be changed into C_p' by a transformation of the form (2), (2) is birational. For let λ, μ be two integers such that $n\lambda + q\mu = 1$. Then

$$y = y^{n\lambda + q\mu} = y'^{\lambda} \cdot S_1(x) = y'^{\lambda} \cdot S_2(x'),$$

where S_1, S_2 are rational functions. This is sufficient to show that x, y are rational in x', y'.

It is readily seen that a suitable transformation (2) will reduce C_p to

$$y^q = \prod_i (x - a_i)^{\alpha_i'},$$

where the (α')'s are subjected to the sole condition of being congruent modulo q to the numbers $n\alpha_i$, n being an arbitrary integer. In particular the (α')'s may thus be replaced by their least residues modulo q, and then the (a)'s remaining will all be critical points. We shall assume that this has already been done, the number of critical points being $r + 2$, so that C_p depends upon $r - 1$ moduli.

If we examine the behavior of y at infinity we find that there is a critical point there corresponding to an exponent $-\sum \alpha_i$. Hence the sum of the exponents corresponding to *all* critical points is divisible by q.

133. Let us assume then that $a_{r+2} = \infty$ so that the equation is in the form

$$y^q = \prod_{i=1}^{r+1} (x - a_i)^{\alpha_i}. \tag{3}$$

As the sum of the (α)'s for all critical points is divisible by q, we may assume that the $r+1$ exponents here indicated are prime to q as well as their sum and are their own least positive residues modulo q. Each critical point counts for $q-1$ branch points of the Riemann surface representing the function $y(x)$ and there are no others. As the surface is q-sheeted, we have $(r+2)(q-1) = 2(p+q-1)$, therefore $p = \frac{1}{2}r(q-1)$.

Any integral of the first kind is of the form

$$\sum_{n=0}^{q-1} \int \frac{R_n(x)}{y^n}\, dx,$$

where the (R)'s are rational functions. If we apply T^k it becomes

$$\sum_n \epsilon^{nk} \int \frac{R_n(x)}{y^n}\, dx.$$

Summing with respect to k it is found that

$$\int \frac{R_n(x)}{y^n}\, dx$$

is of the first kind. Hence at once $R_0 \equiv 0$. Moreover by considering what happens at the critical points we find readily that this last integral is of the form

$$u = \int \frac{\prod_{i=1}^{r+1} (x - a_i)^{\beta_i}}{y^n} \phi(x)\, dx$$

where ϕ is a polynomial. Any other integral is then linearly dependent upon those such as u—a result due to Königsberger.

134. In order that u be of the first kind the following inequalities must be satisfied:

$$(4)\qquad \begin{cases} \beta_i - \dfrac{n\alpha_i}{q} > -1 & (i = 1, 2, \cdots, r+1) \\ \sum \dfrac{n\alpha_i}{q} \sum \beta_i - r' > 0, \end{cases}$$

$r' - 1$ being the degree of ϕ. To take the (β)'s as small as possible is tantamount to changing the degree of ϕ. Denoting as usual by $[m]$ the least integer contained in the positive number m, let us take then $\beta_i = [n\alpha_i/q]$ so that all but the last of (4) will be satisfied. The second may be written

$$r' < \left(\left[\sum \frac{n\alpha_i}{q}\right] - \sum \beta_i\right) + \left(\sum \frac{n\alpha_i}{q} - \left[\sum \frac{n\alpha_i}{q}\right]\right).$$

The second parenthesis is positive and < 1,

$$\therefore \quad \left[\sum \frac{n\alpha_i}{q}\right] - \sum \left[\frac{n\alpha_i}{q}\right] \geqq r' > 0 .$$

Conversely if this inequality is satisfied u is of the first kind whatever the polynomial ϕ of degree $r' - 1$. For it is only necessary to verify the last of (4). Now since neither n nor $\sum \alpha_i$ are divisible by q,

$$\sum \frac{n\alpha_i}{q} - \sum \beta_i - r' > \left[\sum \frac{n\alpha_i}{q}\right] - \sum \left[\frac{n\alpha_i}{q}\right] - r' \geqq 0 ,$$

as was to be proved.

Thus for every n there are r' integrals of the first kind, where

$$r' = \left[\sum \frac{n\alpha_i}{q}\right] - \sum \left[\frac{n\alpha_i}{q}\right].$$

134. When C_p is transformed by T its Jacobi variety undergoes the transformation $u_j' = \epsilon^{n_j} \cdot u_j \quad (j = 1, 2, \cdots, p)$, where $u_1, u_2, \cdots, u_p$ are p independent integrals of the first kind such as u, with n_j corresponding to n. The corresponding value r_j of r' denotes the number of times that the multiplier ϵ^{n_j} is repeated. But if r_j' corresponds to $\epsilon^{-n_j} = \epsilon^{q-n_j}$ and if the (n)'s are all included between *one* and q, then

$$r_j + r_j' = \left[\sum \frac{n_j\,\alpha_i}{q}\right] + \left[\sum \frac{(q - n_j)\,\alpha_i}{q}\right] - \sum \left[\frac{n_j\,\alpha_i}{q}\right] - \sum \left[\frac{(q - n_j)\,\alpha_i}{q}\right] = r .$$

Hence the complex multiplication corresponding to T is of the type which we have studied. The multipliers are the roots of an irreducible equation of degree $q - 1$ whose rth power is the characteristic equation. These multipliers, it is scarcely necessary to point out, are all imaginary, each being a rational function of its conjugate—in fact its inverse. This of course does not allow us to apply without a preliminary discussion the formulas of Chapter II, since the Riemann matrices are by no means the most general of their type. It is nevertheless remarkable that if the critical points are arbitrary the formulas for the indices of the Jacobi variety are the same as for the most general Abelian variety of similar type.

The integer r, equal to the number of critical points decreased by two, will play the same part as in Chapter II, and we observe at once that if $r = 1$, one of the two numbers r_j, r_j' is always zero.

135. Let now ω be any period of u. We have

$$\omega = \sum_{\mu=0}^{r} \epsilon^{n\nu_\mu} (1 - \epsilon^{n\nu_{\mu+1}}) \cdot \int_{x_0}^{a_{\mu+1}} du \qquad (\nu_{\mu_0} = 0).$$

Also

$$\epsilon^{n\nu_\mu}(1 - \epsilon^{n\nu_\mu+1}) = (1 - \epsilon^n)\cdot g_\mu(\epsilon^n),$$

where g_μ is a polynomial with integral coefficients. Hence

$$\omega = (1 - \epsilon^n) \sum_{\mu=0}^{r} g_\mu(\epsilon^n)\cdot \int_{x_0}^{a_{\mu+1}} du.$$

On the other hand

$$\tau_\mu = -(1 - \epsilon^n)\cdot\int_{x_0}^{a_\mu} du - \epsilon^n(1 - \epsilon^{-n})\cdot\int_{x_0}^{a_{\mu+1}} du = (1 - \epsilon^n)\cdot\int_{a_\mu}^{a_{\mu+1}} du$$

is a period, and so is $\epsilon^{nh}\tau_\mu$ as well. The (γ)'s in the sequence designating polynomials with integral coefficients, we have

$$\omega - \gamma_r(\epsilon)\tau_r = (1 - \epsilon^n)\sum_{\mu=0}^{r-1} g'_\mu(\epsilon^n)\cdot\int_{x_0}^{a_{\mu+1}} du$$

$$(g'_\mu = g_\mu, \qquad \mu < r - 1; \qquad g'_{r-1} = g_{r-1} + g_r).$$

This reasoning may be continued until we have finally

$$\omega - \sum_{\mu=1}^{r} \gamma_\mu(\epsilon^n)\tau_\mu = \gamma_0(\epsilon^n)(1 - \epsilon^n)\int_{x_0}^{a_1} du.$$

The left-hand side is a period, hence the other side must be one also. But the corresponding circuit in the x plane can only surround the critical point a_1, hence it is a zero cycle of C_p and $\gamma_0 = 0$. Another way of seeing it is to remark that the second side of the equation like the first must be independent of x_0 and as it is zero for $x_0 = a_1$, it must vanish identically. We have then $\omega = \sum_{\mu=1}^{r}\gamma_\mu(\epsilon^n)\tau_\mu$. If in place of n we had n_j, ϵ^n would have to be replaced by ϵ^{n_j}, whence follows that the period matrix is equivalent to one composed with the arrays,

$$\tau = \| \tau_{j\mu} \| ; \qquad \| 1, \epsilon^{n_j}, \epsilon^{2n_j}, \cdots, \epsilon^{(q-2)n_j} \|$$
$$(j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, r),$$

where

$$\tau_{j\mu} = \int_{a_\mu}^{a_{\mu+1}} du.$$

Remark: It is clear that instead of taking for limits of integration two (a)'s of consecutive indices we could take any two (a)'s provided that the quantities $\tau_{j\mu}$ are not related by a linear equation

$$\sum_\mu \gamma'_\mu(\epsilon^{n_j})\tau_{j\mu} = 0 \qquad (j = 1, 2, \cdots, p).$$

136. *Weierstrass points.* We recall that a point A of an algebraic curve of genus p is said to be a *Weierstrass point* if the excluded orders of infinity for rational point functions of which it is the sole pole do not form the series

$1, 2, \cdots, p$. According to Weierstrass the number of such points is finite and > 0 if $p > 0$ (lacunary theorem). Let t be a variable such that a certain region around the origin in the t plane be in point-to-point correspondence with the vicinity of A on the curve. We may choose p integrals of the first kind $u_1, u_2, \cdots, u_p$, such that near A

$$u_i = t^{s_i}\mathfrak{P}_i(t),$$

where $s_1 < s_2 < \cdots < s_p$, and the $(\mathfrak{P})$'s are holomorphic functions near $t = 0$ and do not vanish there. Of course the choice of the (u)'s is not unique but the (s)'s are perfectly determined and in fact they are the excluded orders for A, which is then a Weierstrass point if and only if

$$m = \sum s_i - \frac{p(p+1)}{2} > 0.$$

The integer m is called the *order* of the point. It is at once obvious that this order is invariant under birational transformations and hence that a birational transformation of the curve into itself simply permutes these points. Hurwitz has shown* that if the curve is not hyperelliptic $m < \frac{1}{2}p(p-1)$, whereas for every Weierstrass point of hyperelliptic curves $m = \frac{1}{2}p(p-1)$.

137. Let us now return to the curves which we are investigating and choose for the r_j integrals belonging to n_j the following:

$$\int \frac{(x-a_i)^{\gamma_j - 1}\prod_{i=1}^{r+1}(x-a_h)^{\beta_h^j}\,dx}{y^{n_j}} \qquad (\gamma_j = 1, 2, \cdots, r_j),$$

and for the variable t relatively to $(a_i, 0)$,

$$t = (x - a_i)^{\frac{1}{q}}.$$

To show that it is suitable observe that in the neighborhood of the point $(a_i, 0)$, y is holomorphic in t, and in fact

$$y = t^{\alpha_i}\mathfrak{P}(t^q),$$

where $\mathfrak{P}(z)$ is holomorphic in z near the origin and does not vanish there. Hence if e, e' are integers such that $e\alpha_i + e'q = 1$ (we shall frequently write $e \equiv 1/\alpha_i$, mod. q, when e satisfies such a relation), we have

$$t = y^e(x-a_i)^{e'}\mathfrak{P}(x-a_i).$$

It is then verified at once that the integral written above has a development near $t = 0$, of the form

$$t^{(\beta_i^j + \gamma_j)q - n_j\alpha_i}\,\mathfrak{P}_1(t^q),$$

*Mathematische Annalen, vol. 41, (1893).

where $\mathfrak{P}_1$ behaves like $\mathfrak{P}$. That this function contains only terms in t^q is seen at once by observing that the effect of T on both t and the integral is merely to multiply them by powers of ϵ.

The exponents $(\beta_i^j + \gamma_j) q - n_j \alpha_i$ form the set of integers $s_1, s_2, \cdots, s_p$ for C_p and the point A_i.

We may apply to C_p a birational transformation such that α_i be replaced by unity and n_j by $n_j' \equiv n_j \alpha_i$, mod. q, $0 < n_j' < q$. Then β_j will be replaced by $[n_j'/q] = 0$, and the set of the (s)'s becomes the set

$$\gamma_j q - n_j' \qquad (\gamma_j = 1, 2, \cdots, r_j; j = 1, 2, \cdots, q - 1).$$

They certainly do not form the set $1, 2, \cdots, p$ if $r > 1$ and the numbers r_j are not all equal. Hence *the critical points are all Weierstrass points when* $r > 1$, *unless the numbers* r_j *are all equal.*

Assume now $r = 1$. Then $\gamma_j = 0$, or 1, and we have to deal with the set $q - n_j'$ $(j = 1, 2, \cdots, p)$ which is up to a factor mod. q the set of the (n)'s. Hence if the set of (n)'s is not congruent mod. q to the set $1, 2, \cdots, p$, the three critical points are Weierstrass points.

138. We shall now apply similar considerations to the proof of a very useful theorem:—*If two curves*, C_p, C_p',

$$y^q = \prod_i (x - a_i)^{\alpha_i}, \qquad y^q = \prod_i (x - a_i')^{\alpha_i'},$$

are birationally equivalent through a transformation S, *this transformation will be of type* (2) *if and only if it transforms some critical point into another.*

The condition is obviously necessary. Let us show that it is sufficient. Assume then that S transforms $A_i(a_i, 0)$ into $A_i'(a_i', 0)$, these two points being both at finite distance, which is not a restriction. Let $u_1, u_2, \cdots, u_p$ be the integrals of No. 137 corresponding to A_i and consider in particular

$$u_p = t^{s_p} \mathfrak{P}(t^q).$$

It is determined up to a constant factor, for the development of $c_1 u_1 + c_2 u_2 + \cdots + c_p u_p$ begins with a term in t^{s_i} if c_i is the first coefficient c not zero. Hence it begins with a term in t^{s_p} only if all the (c)'s except c_p are zero.

Let now (x, y), (x', y') be two corresponding points of C_p, C_p' through S and set $x' - a_i' = t'^q$. The two variables t, t' are obviously holomorphic functions of each other near the origin. Hence

$$t' = t \cdot \mathfrak{P}(t).$$

($\mathfrak{P}$ here as in the sequence designates a function of the type already described.) In making this substitution in u_p it becomes

$$u_p' = t'^{s_p}(a + bt'^q \cdots).$$

This shows that the integral corresponding to s_p for A_i on C_p corresponds to it also for A'_i on C'_p, as might indeed be expected. Now

$$u_p = \int \frac{(x-a_i)^\delta R(x)}{y^n}\,dx, \qquad u'_p = \int \frac{(x'-a'_i)^{\delta'} R'(x')}{y'^{n'}}\,dx'$$

where R, R' are rational functions which neither vanish nor become infinite at a_i, a'_i respectively, and moreover

$$\frac{\delta - n\alpha_i}{q} = \frac{\delta' - n'\alpha'_i}{q} = \frac{s_p}{q} - 1.$$

Near $x = a_i$, $x' = a'_i$, we have then a relation

$$(x-a_i)^{\frac{s_p}{q}-1}\,\mathfrak{P}(x-a_i)\,dx = (x'-a'_i)^{\frac{s_p}{q}-1}\,\mathfrak{P}'(x'-a'_i)\,dx'.$$

When x approaches a_i, x' must approach a'_i; hence if we integrate, the constants of integration must be made equal to zero. Integrating, then raising to the power q/s_p, we obtain

$$(x-a_i)\,\mathfrak{P}_1(x-a_i) = (x'-a'_i)\,\mathfrak{P}'_1(x'-a'_i).$$

This shows that x' is holomorphic in x in the vicinity of $x = a_i$. But there is a relation

$$x' = R(x, y) = \sum_{s=0}^{q-1} R_s(x)\,y^s,$$

where the (R)'s are rational functions. If the (R)'s other than R_0 were $\neq 0$, x' would have an algebraic critical point at a'_i, hence $x' = R_0(x)$. Similarly x is rational in x', and therefore $x' = (ax+b)/(cx+d)$. But also

$$y' = R'(x, y) = \sum_{s=0}^{q-1} R'_s(x)\,y^s.$$

Now y'^q is rational in x' and therefore in x, which requires that of the (R')'s only one, and that one of index > 0, does not vanish. The theorem is therefore proved.

Remarks: I. If the equation of S for y is

$$y' = y^\lambda \cdot R(x),$$

it is seen that its effect upon the integral u_j corresponding to n_j is to transform it into an integral corresponding to λn_j, that is, all the (n)'s are multiplied by λ, mod. q. But $s_p \equiv -n_p\alpha_i \equiv -n'_p\alpha'_i$, mod. q,

$$\therefore\quad \frac{n'_p}{n_p} \equiv \frac{\alpha_i}{\alpha'_i} \equiv \lambda, \text{ mod. } q.$$

II. The equations of the transformation T' of C'_p corresponding to T on C_p

are $x = x'$, $y = \epsilon^\lambda y'$, that is, by virtue of S the cyclic transformations apparent for each curve are transformed into powers of each other. If we recall then the invariant meaning given to x in No. 132 relatively to birational transformations we see at once that S transforms the set of (A)'s into the set of (A')'s. Hence *if a birational transformation changes a single point A_i into an A'_i it does so for all of them.*

139. A particularly interesting case is that where C_p and C'_p coincide. According to the remark just made, *a birational transformation of C_p into itself either permutes the set of (A)'s with a similar set having not a single point in common with the first and corresponding to a cyclic transformation of order q not a power of T, or else it maintains the set in question completely invariant.* Assume then S to be of the second type and let ν be its order. Its equations for a suitable choice of x will assume the form

$$x' = \eta x, \qquad y' = y^\lambda R(x); \qquad (\eta = e^{\frac{2k\pi i}{\nu}}; \qquad \lambda^\nu \equiv 1, \text{ mod. } q).$$

Incidentally if $\lambda > 1$, ν is *not prime* to $q - 1$. If a_i is a critical point, $\eta^s a_i$ is one also, and the corresponding exponent α can be taken to be $\lambda^s \alpha_i$. Also if one of the points $x = 0$, $x = \infty$, is critical, it will be maintained invariant by S, hence then (Remark I, No. 138), $\lambda = 1$. There are two distinct possibilities:

(*a*) $\lambda \not\equiv 1$, mod. q. C_p can be reduced to

$$y^q = \phi(x)\cdot[\phi(\eta^{-1}x)]^\lambda \cdots [\phi(\eta^{1-\nu}x)]^{\lambda^{\nu-1}}$$

where ϕ is a polynomial with $\phi(0) \neq 0$. The critical points of this curve are not completely arbitrary. As our investigation will be limited to curves with critical points as arbitrary as possible for each type the only curve of this nature that we shall have to consider is the curve with three critical points, and $\nu = 3$, reducible to:

$$y^q = (x-1)(x-\eta)^\lambda(x-\eta^2)^{\lambda^2}, \qquad (\lambda^3 = 1, \text{ mod. } q;\ \eta = e^{\frac{2\pi i}{3}}),$$

and which presents itself only when $q - 1$ is a multiple of *three*. It may be found directly that the equations of S are

$$x' = \eta x, \qquad y' = \eta^{\frac{1+\lambda+\lambda^2}{q}} y^\lambda.$$

(*b*) $\lambda \equiv 1$, mod. q. C_p can then be reduced to

$$y^q = x^\alpha \prod_i (x^\nu - a_i^\nu)^{\alpha_i}.$$

The only curve of this type with arbitrary critical points is reducible to one of the two hyperelliptic curves

$$y^q = \frac{x^2 - a^2}{x^2 - b^2}, \qquad y^q = x^2 - a^2.$$

For both curves, S is the ordinary binary transformation characteristic of hyperelliptic curves. This transformation is permutable with T.

Remark: It is easy to show that if S maintains every A invariant then it is a T^k. For its equations must be

$$x' = x, \qquad y' = y \cdot R(x).$$

By direct substitution in the equation of C_p we find at once $R^q = 1$, hence $R = \epsilon^k$ which proves our assertion.

140. We can now show that if a transformation T' of order q has also one of the (A)'s for coincidence point then $T' = T^k$. In other words *a single coincidence point determines the rest of them and the corresponding cyclic group of order q as well.* For if we choose x properly the equations of T' will be

$$x' = \epsilon^n x, \qquad y' = y^\lambda \cdot R(x).$$

Since T' is of order q we must have $\lambda^q \equiv 1$, mod. q, and therefore according to Fermat's theorem, $\lambda \equiv 1$, mod. q, and we may take in fact $\lambda = 1$. C_p will then be reducible to the form

$$y^q = x^\alpha \prod_i (x^q - a_i^q)^{\alpha_i},$$

with α not divisible by q, if we assume as we may that the common coincidence point of T and T' is at the origin. By direct substitution it is found that we must have $R(x) = \epsilon^{n\alpha/q}$ with the condition that $n\alpha \equiv 0$, mod. q, if $T'^q = 1$. Hence we may take $n = 0$, and the equations of T' are finally $x' = x$, $y' = \epsilon^k \cdot y$ which shows that $T' = T^{-k}$ as was to be proved.

As a corollary if S permutes the (A)'s among themselves, STS^{-1} being a transformation such as above is a T^k, hence $ST = T^k \cdot S$. From this follows readily $S^j \cdot T = T^{k^j} \cdot S^j$. This shows that the group generated by the products of the powers of S and T is of order $q\nu$, where ν is the order of S. To obtain the exact relations existing between the transformations observe that $S^\nu \cdot T = T = T^{k^\nu} \cdot S^\nu$, hence $k^\nu \equiv 1$, mod. q. Moreover $k \not\equiv 1$, mod. q, else S would be permutable with T and this can only be when C_p is hyperelliptic and S is its ordinary binary transformation. This results from the fact proved in Chapter III, that the only cyclic transformations of the Jacobi variety of C_p permutable with T is the ordinary transformation, $u_i' = -u_i$ $(i = 1, 2, \cdots, p)$, to which corresponds only the ordinary binary transformation present in hyperelliptic curves, and none at all if the curve is not hyperelliptic. This case being set aside for the present, we must take for ν a root of the congruence other than one.

This being assumed, we find first

$$(S^j T^i)^n = T^l \cdot S^{nj}; \qquad l = ik^j \frac{(k^{nj} - 1)}{(k^j - 1)}.$$

It follows at once that in all cases $S^j\, T^i$ is either of order ν or of order q. It is certainly of order ν when: (a) there are no relations $S^\alpha = T^\beta$, $\alpha < \nu$; (b) $j \neq 0$; (c) k is a primitive root of its congruence.

141. Torelli has proved a proposition of which we shall make some very interesting applications:* *Two algebraic curves of same genus with identical period matrices as to sets of normal integrals of the first kind are birationally equivalent.*

It follows at once that if the period matrices of two sets of integrals of the first kind are equivalent the curves are still birationally equivalent. However of more interest to us is this immediate corollary: If a given algebraic curve possesses two distinct sets of integrals of the first kind with *identical* period matrices it possesses a birational transformation into itself by which

*Rendiconti dei Lincei (1913). [Added in 1922: Rosati has shown in the Palermo Rendiconti, vol. 44 (1920), that Torelli's theorem requires that the periods correspond to retrosections.—As a matter of fact, in the cases of interest in the sequence this condition is actually fulfilled, and moreover Torelli's theorem is not essential as I proceed to show.

Let y_1, $y_2 = T\cdot y_1$, $y_3 = T^2\cdot y_1$, $\cdots$, be the determinations of y. To each pair of loops aa_1, $aa_{\mu+1}$, of the x plane, corresponds in a well-known manner a cycle δ_k^μ of C_p, running entirely (save perhaps in the vicinity of a_1 and $a_{\mu+1}$) in the sheets y_k, y_{k+1} ($y_{q+1} = y_1$), of the Riemann surface of $y(x)$, and $\delta_k^\mu = T\cdot\delta_{k-1}^\mu$. The $2p$ cycles δ_k^μ ($\mu = 1, 2, \cdots, r$; $k = 1, 2, \cdots, q-1$) constitute precisely a fundamental system corresponding to the period matrix of No. 135.—Any birational transformation of the Jacobi variety, to occur later, shall have the property that *it induces permutations of the* (u) *'s and of the cycles* δ_1^μ, δ_2^μ, $\cdots$, *for each* μ, *of common order* $\neq 0$, *leaving the period matrix invariant.* Up to an ordinary transformation, this completely characterizes U, and I say that *correspondingly there is a birational transformation of* C_p *into itself, which is not a power of* T.

Let $C'_p = U\cdot C_p$. To the coincidence points $A_i\,(a_i, 0)$, of T on C_p, correspond those A'_i of $T' = UTU^{-1}$ on C'_p, the indices being so chosen that if α'_i is the same for A'_i as α_i for A_i, the ratios α'_i/α_i are all congruent mod. q. This being done, we readily define a birational transformation S of C_p into C'_p such that $A'_i = S\cdot A_i$, and that the cycles $S\delta_1^\mu$, $S\delta_2^\mu$, $\cdots$, are cyclically permuted by T'. Observe that any birational transformation of order q of C'_p, with the (A')'s for coincidence points, is necessarily a T'^h (No. 140). Now the (u)'s may be defined, up to a constant factor, by the nature of their expansions at a critical point, whence follows readily that their transformed by U on C'_p play the same part for T' as the (u)'s for T (i.e., T' merely multiplies them by constants). On considering the periods with respect to the cycles $U\cdot\delta_k^\mu$, and recalling the assumptions as to U, we see that they cannot be the same as the cycles $S\cdot\delta_k^\mu$ or $T'^hS\cdot\delta_k^\mu$, of same indices, for the first are not cyclically permuted by T', while the last are. Hence $U \neq ST'^h$, and $S^{-1}U$ is a birational transformation of C'_p into itself not a T'^h, and as there is a similar one for C_p, our assertion is proved.

We may also verify that the Rosati condition is fulfilled. For each of the sets of $2p$ cycles $U\cdot\delta_k^\mu$, $S\cdot\delta_k^\mu$ ($k < q$), of C'_p, has this property: If the Riemann surface of C'_p is cut open along them, it is reduced to a two-cell, and these cells are reducible to each other by a homeomorphism, wherein the cuts $U\delta_k^\mu$, $S\delta_k^\mu$ correspond to one another. Moreover there are integrals of the first kind with identical period matrices with respect to these cycles. From this follows readily enough the existence of two distinct sets of retrosections, with identical canonical period matrices, hence Rosati's condition is verified, and as previously C'_p possesses a birational transformation into itself.

Observe that from the discussion of No. 141 it will appear that unless the curve is hyperelliptic, the order of the birational transformation of the curve is the same as that of U.]

the integrals of one system are transformed into those of the other. If then $u_1, u_2, \cdots, u_p$ and $u'_1, u'_2, \cdots, u'_p$ are the two sets of integrals, $M(x, y)$ any point of the curve, $M'(x', y')$ its transformed through S, we have

$$u'_j(x', y') = u_j(x, y) + \delta_j \qquad (j = 1, 2, \cdots, p),$$

where the (δ)'s are constants. Since the two sets of integrals are distinct the algebraic correspondence defined by these relations is *singular* and therefore $S \neq 1$.

In particular if the period matrix is changed identically into itself by a certain equivalence the curve possesses a corresponding birational transformation.

We have already remarked that the transformation of the Jacobi variety defined by

$$u_j(x', y') = -u_j(x, y) + \delta_j \qquad (j = 1, 2, \cdots, p)$$

determines a birational transformation of the curve only when the latter is hyperelliptic. If $u_j(x', y') = u_j(x, y) + \delta_j$ were to determine a birational transformation of the curve, M and M' would be distinct points of a linear series of order and dimension one and therefore $p = 0$. Hence, except for the ordinary transformation possessed by hyperelliptic curves, to each birational transformation U of a curve of genus $p > 0$ corresponds a non ordinary transformation of its Jacobi variety.—Under the following form this result will be found very useful: *If to U of C_p, non hyperelliptic, corresponds an ordinary transformation of the Jacobi variety, U reduces to the identity.*

142. Returning to the C_p which we are investigating we shall show below that when $r > 1$, and the (a)'s are arbitrary, then $1 + h = q - 1$, where h is the index of multiplication of the Jacobi variety. Exception must be made of the case where $r = 2$ and the integers r_j are all equal to unity. Save in that special case which shall be fully examined in its place, the complex multiplications of the variety are then all linearly dependent upon those determined by the powers of T, and therefore (No. 119) the only non ordinary cyclic transformations of the variety are the powers of T. We shall see that if C_p is hyperelliptic we are in the exceptional case. Thus, save in the exceptional case, if $r > 1$ the total group of C_p is the obvious cyclic group of order q, for otherwise there would have to exist non ordinary cyclic transformations of the Jacobi variety other than the powers of T.

It follows that when the points $A_i\ (a_i, 0)$ are arbitrary and $r > 1$ there is no analogous set distinct from them on C_p, hence any transformation of the curve into itself must maintain them invariant and therefore it is of type (2).

143. Let us show that when $r > 1$ it is not possible that of the two numbers r_j, r_{q-j}, one be always zero. For with a suitable choice of integrals of the

first kind the period matrix would take the form

$$\begin{Vmatrix} \omega, & 0, & 0, & \cdots, & 0 \\ 0, & \omega, & \cdot & \cdots, & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdot & \cdots, & \omega \end{Vmatrix},$$

$$\omega = \| 1, \epsilon^{n_j}, \cdots, \epsilon^{(q-2)n_j} \| \qquad \left(j = 1, 2, \cdots, \frac{q-1}{2}\right),$$

and depends upon no arbitrary constants whereas as we know it should depend upon $r - 1 > 0$ of them.

144. *Hyperelliptic curves.* The curve C_p being assumed hyperelliptic let S be its ordinary binary transformation. It transforms the point (x, y) of C_p into a point (x', y') such that

$$\int \prod_i (x - a_i)^{\beta_i - \frac{n\alpha_i}{q}} dx$$

changes in sign when x is replaced by x'. Dividing two such differential expressions, then raising to the qth power we obtain a relation

$$\prod_i (x - a_i)^{\delta_i} = \prod_i (x' - a_i)^{\delta_i} \qquad (\delta_i \text{ integer})$$

It shows that when x approaches one of the (a)'s, x' approaches another. Hence S is of type (2) and by a proper choice of x we shall have merely $x' = -x$. The equations of the curve will then be

$$y^q = x^\alpha \prod_i (x^2 - b_i^2)^{\alpha_i}$$

As we must have $y' = y^n \cdot R(x)$, we find by direct substitution $n = 1$, $R = (-1)^\alpha$, and S will have for equations

$$x' = -x, \qquad y' = (-1)^\alpha \cdot y.$$

The only hyperelliptic curves with unrestricted critical points are reducible to one of the following two:

$$y^q = x^2 - a^2,$$

$$y^q = \frac{x^2 - a^2}{x^2 - b^2}.$$

In the first case where $r = 1$, we have $\alpha_1 = \alpha_2 = 1$ and the integers r_j and n_j are determined by $[2n_j/q] - r_j \geqq 0$ which shows that n_j must be $> q/2$ in order that $r_j = 1$. Hence n_j takes the values $p + 1, p + 2, \cdots, 2p$ and the period matrix is at once seen to be equivalent to

$$\| 1, \epsilon^j, \epsilon^{2j}, \cdots, \epsilon^{(q-2)j} \| \qquad (j = 1, 2, \cdots, p).$$

For $r = 2$ the curve may be reduced to such a form that $\alpha_1 = \alpha_2 = 1$,

$\alpha_3 = q - 1$. Hence

$$\left[\frac{n_j(q+1)}{q}\right] - \left[\frac{n_j(q-1)}{q}\right] - r_j = 1 - r_j \geqq 0 .$$

Hence n_j can take all the values $1, 2, \cdots, p$ and to each corresponds exactly *one* integral, the period matrix being composed with:

$$\| \tau_{j1}, \tau_{j2} \| , \qquad \| 1, \epsilon^j, \cdots, \epsilon^{(q-2)j} \| \qquad (j = 1, 2, \cdots, p).$$

§ 2. Curves with three critical points

145. Our next object is the study of the C_p whose $r = 1$, and which is reducible to

$$y^q = (x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2}.$$

Since $2p = q - 1$, we may assume $q > 3$, for, if $q = 3$, we have to deal with elliptic curves which offer no great interest.

Let g be a primitive root of q and set $n_j \equiv g^{e_j}$, mod. q. The period matrix is equivalent to:

$$\| \epsilon^{g^{e_j}}, \epsilon^{g^{e_j+1}}, \cdots, \epsilon^{g^{e_j+2p-1}} \| \qquad (j = 1, 2, \cdots, p).$$

In conformity with Chapter II, § 3, we must first ask ourselves if there exists a subgroup of order $\nu = p/p'$ of the cyclic group of the equation $(x^q - 1)/(x - 1) = 0$, maintaining invariant the multipliers $\epsilon^{g^{e_j}}$. This problem is equivalent to that of determining if there exists a factor p' of p such that if we add $2p'$ to one of the (e)'s we get another, mod. $(q - 1)$. Assume that such is the case. The period matrix may be put in the form

$$\| \epsilon^{g^{e_j}}, \epsilon^{g^{e_j+2p'}}, \cdots, \epsilon^{g^{e_j+2(\nu-1)p'}}, \epsilon^{g^{e_j+1}}, \epsilon^{g^{e_j+1+2p'}} \cdots \| \qquad (j = 1, 2, \cdots, p).$$

Let us range the integrals of the first kind in such an order that $u_{j+kp'}$ $(k \leqq \nu - 1)$ corresponds to $e_j + 2kp'$. We recognize then that under the assumptions made if we permute cyclically the columns of order $k\nu + 1$, $k\nu + 2, \cdots, (k+1)\nu$ $(k = 0, 1, \cdots, 2p' - 1)$, in the period matrix in the form just written, and permute at the same time cyclically the rows $j, j + p', \cdots, j + (\nu - 1)p'$ $(j = 1, 2, \cdots, p')$, the matrix is unchanged. Hence (No. 141), C_p possesses a birational transformation S of order ν. The genus of the involution defined by a given point and its $(\nu - 1)$ transformed through the powers of S is easy to obtain. For if $\eta = e^{2\pi i/\nu}$, S multiplies by η^k the p' integrals

$$u_j + \eta^k u_{j+p'} + \cdots + \eta^{(\nu-1)k} u_{j+(\nu-1)p'} \qquad (j = 1, 2, \cdots, p').$$

Hence the multipliers of the multiplication defined by S on the Jacobi variety are composed of the powers of η, unity included, taken each p' times. There are then exactly p' integrals of the first kind maintained invariant by S,

which shows that p' is the required genus. Since the involution defined by T is of genus *zero,* no power of S can be a T^k. Let now (x, y) be any point of C_p, and (x', y') its transformed by S. This transformation permutes u_j with $u_{j+p'}$, whence at least three relations such as

$$(x - a_1)^{\gamma_1}(x - a_2)^{\gamma_2}\,dx = (x' - a_1)^{\gamma'_1}(x' - a_2)^{\gamma'_2}\,dx'.$$

If we divide two of them by each other we obtain a relation

$$(x - a_1)^{\delta_1}(x - a_2)^{\delta_2} = (x' - a_1)^{\delta'_1}(x' - a_2)^{\delta'_2},$$

the exponents being rational. From this follows that if x tends towards one of the critical points, x' must tend towards another.

Let us denote as before the critical points by A_1, A_2, A_3 and assume first that S maintains one of them, say A_1, invariant. Then the integer λ of No. 139 must be equal to *unity,* mod. q, and the curve is reducible to the form $y^q = x^\alpha(x^2 - a^2)$. It is therefore hyperelliptic. Let S' be its ordinary binary transformation. SS' maintains the (A)'s invariant, hence it is a T^k and therefore $S = T^k S'$, which is absurd for $T^k S'$ determines an involution of genus *zero* while S determines one of genus $p' > 0$.

We conclude then that S permutes cyclically the critical points, and that $\lambda^3 \equiv 1$, mod. q. C_p is therefore reducible to the curve

$$y^q = (x - 1)(x - \eta)^\lambda(x - \eta^2)^{\lambda^2}; \qquad \eta = e^{\frac{2\pi i}{3}}$$

of No. 139, the transformation S being of order *three,* with equations

$$x' = \eta x, \qquad y' = \eta^{\frac{1+\lambda+\lambda^2}{q}}\cdot y^\lambda.$$

This curve which we shall denote by $C_{3p'}$ exists only if $q - 1$ is divisible by three. When $q > 3$, the exponents $1, \lambda, \lambda^2$ are distinct and the curve is certainly not hyperelliptic.

Referring to Chapter II, § 3, we may affirm that the invariants of the Jacobi variety when $r = 1$ are given by

$$1 + h = 2(1 + k) = 2p = q - 1$$

unless we deal with $C_{3p'}$ when we have

$$1 + h = 2(1 + k) = 6p = 3(q - 1).$$

In this last case the period matrix is isomorphic to one of type

$$\begin{Vmatrix} \omega, & 0, & 0 \\ 0, & \omega, & 0 \\ 0, & 0, & \omega \end{Vmatrix},$$

where ω is pure and of genus $p' = p/3$.

146. The curve $C_{3p'}$ may be reduced to a particularly interesting form. For since $\frac{1}{3}(q-1)$ is an integer, q is decomposable in a unique manner in the domain $K(\sqrt{3})$, hence there are two relatively prime positive integers m, n, such that $q = m^2 - mn + n^2$. The curve represented in homogeneous coordinates by $x^m y^n + y^m z^n + z^m x^n = 0$ is invariant under the collineation group of order $3q$ generated by the two operations

$$x' = y, \qquad y' = z, \qquad z' = x;$$
$$x' = \epsilon^m x, \qquad y' = \epsilon^n y, \qquad z' = z.$$

Let γ, δ be two integers such that $m\gamma + n\delta = 1$. If we apply to $x^m y^n + x^n + y^m = 0$ the birational transformation

$$x = x'^{\delta} y'^{m}, \qquad y = x'^{-\gamma} y'^{n}$$

whose inverse is

$$x' = x^n y^{-m}, \qquad y' = x^{\gamma} y^{\delta}$$

we obtain

$$y'^{q} = - x'^{-\delta m - \gamma(m-n)} \cdot (1 + x').$$

To prove that this is the curve $C_{3p'}$ we observe first that

$$m^2 - mn + n^2 = q = q(m\gamma + n\delta),$$
$$\therefore \quad m(m - n - q\gamma) = -n(n - q\delta)$$

and since m and n are relatively prime, there is an integer t such that

$$m - n - q\gamma = tn, \qquad n - q\delta = -tm,$$

whence

$$\gamma = \frac{m - n(1+t)}{q}, \qquad \delta = \frac{n + tm}{q};$$
$$\therefore \quad -m\delta - \gamma(m-n) = -(1+t).$$

The three exponents α_i, corresponding to the curve obtained, can therefore be taken to be $1, t, -(1+t)$. Now $nt \equiv m - n$, mod. q,

$$\therefore \quad n(1 + t + t^2) \equiv m^2 - mn + n^2 \equiv 0, \text{ mod. } q.$$

But n may be assumed $< m$, and the relation which defines them shows that n^2 is less than q and therefore prime to it. It follows that $1 + t + t^2$ is divisible by q, or $t^3 \equiv 1$, mod. q, so that t is either the integer λ or λ^2, mod. q, for $t \equiv 1$, mod. q, would mean that either q is 3, or n^2 is divisible by q. The curve which we have obtained corresponds then to the three exponents $1, \lambda, \lambda^2$ and in the case $r = 1$, this suffices to establish that it is birationally equivalent to $C_{3p'}$.

The two simplest curves $C_{3p'}$ have been considered at length by Klein $(q = 7)$, and Virgil Snyder $(q = 13)$, under the form

$$x^3 y + y^3 z + z^3 x = 0$$
$$x^4 y + y^4 z + z^4 x = 0$$

and the invariants of their Jacobi variety have been directly computed by Scorza.*

147. The consideration of the Weierstrass points will be useful for the problem which will occupy us next. Let s_i^h be the value of the integer s_i of No. 136 for A_h. We find at once

$$s_i^1 + s_i^2 + s_i^3 = \left(\beta_1^i + \beta_2^i + \beta_3^i - n_i \frac{(\alpha_1 + \alpha_2 + \alpha_3)}{q} \right) q + 3q.$$

In expressing that u_i is finite at infinity we find that the first term at the right $< -q$, hence the left side is $< 2q$. But $\alpha_1 + \alpha_2 + \alpha_3$ is divisible by q. Hence this left side, which is positive, is a multiple of q, and therefore is exactly equal to q, that is $s_i^1 + s_i^2 + s_i^3 = q$. Hence, if m_h is the order of the point A_h,

$$\begin{aligned} m_1 + m_2 + m_3 &= \sum_{i=1}^{p} (s_i^1 + s_i^2 + s_i^3) - \frac{3p(p+1)}{2} \\ &= pq - \frac{3p(p+1)}{2} = \frac{p(p-1)}{2}. \end{aligned}$$

148. We have seen that for the curves other than $C_{3p'}$, $1 + h = q - 1 = 2p$. Hence (No. 142) the total group of these curves is the cyclic group of order q generated by T, except in the hyperelliptic case when it is of order $2q$. It remains to examine $C_{3p'}$. We propose to show that *when* $q > 7$ *the total group of* $C_{3p'}$ *is the group of order* $3q$ *generated by the cyclic operations* T *of order* q *and* S *of order* 3.

We have seen that $ST = T^\mu S$, where $\mu^3 \equiv 1$ but $\mu \not\equiv 1$, mod. q, and therefore the group generated by S, T, is indeed of order $3q$. Moreover either μ or μ^2 is the integer repeatedly denoted by λ. Since there are no relations $S^\alpha = T^\beta$, $S^i T^k$ $(i = 1, 2)$ is of order three (No. 140).

149. Let $\sum$ be a birational transformation of $C_{3p'}$ into itself, not an $S^i T^k$, and let ν be its order. It induces in the Jacobi variety one of equal order, $\sum'$, for when either one is the identity so is the other (No. 141). Hence among the multipliers of $\sum'$ is found at least one primitive ν-th root of unity. On the other hand these multipliers satisfy the characteristic equation, which is of degree $q - 1$, and as we know (No. 93), is reducible in $K(\epsilon)$, its left side becoming there the product of $2p'$ cubic factors.—Now the primitive ν-th roots satisfy an equation whose degree is the Euler function $\varphi(\nu)$, and which is irreducible in the rational domain. Hence the roots of this equation satisfy the characteristic equation as well, and $\varphi(\nu) \leqq q - 1$. $\therefore$ $\nu = q, 2q$, or else it is prime to q. But in this last case the equation in the ν-th primitive

* See Klein—Fricke, *Vorlesungen über elliptische Modulfunctionen*, vol. 1, p. 701; Snyder, American Journal of Mathematics, vol. 30, (1908); Scorza, Atti dell' Accademia Gioenia (1917).

roots is irreducible in $K(\epsilon)$ (Kronecker). Hence one of the cubic factors above has for roots all the primitive ν-th roots, whence then $\varphi(\nu) \leqq 3$, $\nu = 2, 3, 4, 6$. Thus finally ν can only have the values $2, 3, 4, 6, q, 2q$.

The case $\nu = 2q$ may be excluded at once for then the multipliers are necessarily the quantities $-\epsilon^{n_j}$ and $\sum'^q$ is the ordinary multiplication present only when the curve is hyperelliptic. There remain then only the possibilities $\nu = 2, 3, 4, 6$ or q. Through $\sum$ the points A_1, A_2, A_3 are transformed into new points A'_1, A'_2, A'_3, for by the discussion of No. 140 it is readily seen that $C_{3p'}$ possesses no other transformations than an $S^i\, T^k$ leaving the set of (A)'s invariant. These new points are coincidence points for the transformation of order q, $\sum T \sum^{-1}$. Let A^k_i be the transformed of A'_i by T^{k-1}, or of A_i by $T^{k-1} \sum$. The (A^k)'s are also coincidence points for a certain transformation of order q, and I say that an A^k can be neither an A^h nor an A. For otherwise $\sum^{-1} T^{k-h} \sum$ would transform an A into another, and therefore $\sum^{-1} T^{k-h} \sum = S^j\, T^k$. But if $j \neq 0$ this is impossible for the two transformations are of different orders q, and three, while if $j = 0$, it leads to $\sum T^k \sum^{-1} = T^{k-h}$, again impossible whether $k \neq h$, as the two substitutions have then different coincidence points, or still worse $k = h \neq 0$. Thus the existence of $\sum$ brings as a corollary that of $(q+1)$ sets of three Weierstrass points. The sum of the orders of the (A^k)'s is obviously equal to the sum of the orders of the (A)'s, that is, to $p(p-1)/2$. The sum of the orders of all the Weierstrass points thus obtained is $(q+1)p(p-1)/2 = p(p^2-1)$. But this is the sum of the orders of all the Weierstrass points (Hurwitz), hence $C_{3p'}$ can have no others. Thus the Weierstrass points are grouped in sets of three and any birational transformation $\sum$ merely permutes the sets among themselves. This follows from the fact that if $\sum$ permutes for example A_1 with A^1_1, A^1_1 is critical for a definite transformation of order q, $\sum T \sum^{-1}$, whose cyclic group is uniquely defined by A^1_1, and hence also the corresponding set of three coincidence points to which $\sum A_2$ and $\sum A_3$ necessarily belong. This set can only be A^1_1, A^1_2, A^1_3. Henceforth the set of (A^k)'s will be denoted by (A^k).

150. I say that S permutes at least two sets (A^k). For if it maintained them all fixed, ST would permute q of them cyclically which is impossible as its order is three. Assume then that S permutes (A^{k+1}) with some other set. The transformation $U = \sum^{-1} T^{-k} S T^k \sum$ which is of order three permutes cyclically (A) with two other sets, say (A^1), (A^2) in the order named. On the other hand the number of sets is $q+1$ which is prime to three, hence S must maintain fixed at least one set other than (A), say (A^{h+1}). Then $T^{-h} S T^h$ is a transformation of order three maintaining invariant (A) and (A^1) and it may be assumed without inconvenience to be S itself. Finally if $V = UT$, we have $V(A) = UT(A) = (A^1)$, $V(A^1) = UT(A^1) = U(A^2)$

$= (A)$. It follows that V^2 maintains (A) invariant and can only be of order one, three, or q and V therefore of order $2, 3, 6$, or q since $2q$ is excluded. It is also obviously not of order 3 or q. Hence V is of order 2 or 6.

It is at once verified that the effect of V on the point A_1 is expressed by one of the relations

$$VSA_1 = SVA_1, \qquad VSA_1 = S^2 VA_1.$$

Hence either $VS = SVT^k$, or $VS = S^2 VT^k$. If $k \neq 0$ we must have one of the relations

$$V^{-1} S^{-1} VS = T^k, \qquad V^{-1} S^{-2} VS = T^k$$

which is impossible for T^k maintains (A) alone fixed, while the other substitutions maintain both (A) and (A') fixed. Thus, *if there is a transformation $\sum$ of $C_{3p'}$, not an $S^i T^k$, there is one V of order* 2 *or* 6, *such that VT^{-1} is of order* 3, *and that moreover either $VS = SV$, or $VS = S^2 V$.*

151. Let us examine now the effect of the birational transformations $S^i T^k$ on the integrals of the first kind. It is seen at once that they transform a linear combination $au_j + bu_{j+p'} + cu_{j+2p'}$ into one of the same type. We have there $3q$ birational transformations and if we range the integrals in suitable order, their transformations will be represented by arrays such as

$$\begin{Vmatrix} B_1, & 0, & \cdots, & 0 \\ 0, & B_2, & \cdots, & 0 \\ \cdot & \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot & \cdots, & B_{p'} \end{Vmatrix}$$

where B_j is itself an array of one of the three following types

$$\begin{Vmatrix} \epsilon^{n_j}, & 0, & 0 \\ 0, & \epsilon^{\lambda n_j}, & 0 \\ 0, & 0, & \epsilon^{\lambda^2 n_j} \end{Vmatrix}, \quad \begin{Vmatrix} 0, & \epsilon^{n_j}, & 0 \\ 0, & 0, & \epsilon^{\lambda n_j} \\ \epsilon^{\lambda^2 n_j}, & 0, & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 0, & 0, & \epsilon^{n} \\ \epsilon^{\lambda n_j}, & 0, & 0 \\ 0, & \epsilon^{\lambda^2 n_j}, & 0 \end{Vmatrix},$$

corresponding to T^j, ST^j, $S^2 T^j$, respectively. The array of the (B)'s represents also a complex multiplication. Each set contains q multiplications of which $q - 1$ are independent and between the three sets of $q - 1$ independent multiplications thus obtained there are no linear relations. Since $1 + h = 3(q - 1)$, these multiplications form a base. Therefore any multiplication can be represented by an array such as that of the (B)'s with now any one of the (B)'s of the form

$$\begin{Vmatrix} g_1(\epsilon), & g_2(\epsilon), & g_3(\epsilon) \\ g_3(\epsilon^{\lambda}), & g_1(\epsilon^{\lambda}), & g_2(\epsilon^{\lambda}) \\ g_2(\epsilon^{\lambda^2}), & g_3(\epsilon^{\lambda^2}), & g_1(\epsilon^{\lambda^2}) \end{Vmatrix},$$

the (g)'s being polynomials with rational coefficients. For example, B_j is obtained when ϵ is replaced by ϵ^{n_j}.

152. Let us assume in particular that we are dealing with the complex multiplication defined by the birational transformation V of No. 150, and let us represent the typical B_j just written by

$$\left\| \begin{matrix} a_1, & a_2, & a_3 \\ b_1, & b_2, & b_3 \\ c_1, & c_2, & c_3 \end{matrix} \right\| .$$

If we express the fact that $VS = SV$ or $S^2 V$ we find that this array is necessarily of one of the two forms*

$$\left\| \begin{matrix} a, & b, & c \\ c, & a, & b \\ b, & c, & a \end{matrix} \right\| , \qquad \left\| \begin{matrix} a, & b, & c \\ b, & c, & a \\ c, & a, & b \end{matrix} \right\| .$$

Finally the multipliers are roots of one of the two equations

$$\left\| \begin{matrix} a-x, & b, & c \\ c, & a-x, & b \\ b, & c, & a-x \end{matrix} \right\| = 0, \qquad \left\| \begin{matrix} a-x, & b, & c \\ b, & c-x, & a \\ c, & a, & b-x \end{matrix} \right\| = 0.$$

153. What are these multipliers? *When V is of order two,* they can only be $+1$ and -1, taken one p' times and the other $2p'$ times in the set of p multipliers, or else -1 taken $3p'$ times. But this last case may be set aside as it presents itself only for hyperelliptic curves. Similarly I say that $+1$ cannot be taken $2p'$ times. For then V would leave invariant $2p'$ integrals of the first kind, hence it would determine an involution of order *two* and genus $2p'$ on $C_{3p'}$, involution which must have $2p - 2(2\cdot 2p' - 2) = 2 - 2p' \geqq 0$ coincidences, which is impossible unless $p' = 1$, $q = 7$. Hence except for this last case when $C_{3p'}$ is Klein's quartic, if V is of order *two*, there are p' multipliers equal to $+1$, and $2p'$ equal to -1. The numbers a, b, c above are numbers of the domain $K(\epsilon)$ and when we replace ϵ by ϵ^k we do not change the roots of the equations at the end of No. 152, if they are rational or roots of unity of degree prime to q. Hence these equations will all have -1 for double root and $+1$ for simple root. The sum of these roots is -1 and their product $+1$.

154. *When V is of order* 6, the multipliers can only be $1, \eta^{\frac{1}{2}}, \eta^{-\frac{1}{2}}$, or $-1, \eta^{\frac{1}{2}}, \eta^{-\frac{1}{2}}$, taken each p' times $(\eta = e^{2\pi i/3})$. The first possibility can again be set aside, for then there would be on the curve an involution of order 6 and genus p', with $2p - 2 - 6(2p' - 2) = 10 - 6p'$ coincidences, which requires here also $p' = 1$, $q = 7$. The second and only possible set of multipliers are the distinct roots of $x^3 + 1 = 0$. Their sum is *zero* and their product -1.

* See Klein-Fricke, loc. cit. p. 704, for a similar computation corresponding to $q=7$, $p'=1$.

155. We can now show that to V there cannot correspond a type array

$$\begin{Vmatrix} a, & b, & c \\ c, & a, & b \\ b, & c, & a \end{Vmatrix}$$

for any B. For if $V^2 = 1$, the condition as to the sum of the multipliers gives at once $3a = -1$. On the other hand VT^{-1} must be of order three. But to this transformation corresponds an array of (B)'s of which a typical one is

$$\begin{Vmatrix} a\epsilon, & b\epsilon, & c\epsilon \\ c\epsilon^{\lambda}, & a\epsilon^{\lambda}, & b\epsilon^{\lambda} \\ b\epsilon^{\lambda^2}, & c\epsilon^{\lambda^2}, & a\epsilon^{\lambda^2} \end{Vmatrix}.$$

The corresponding multipliers which can only be $1, \eta, \eta^2$ are roots of

$$\begin{vmatrix} a\epsilon - x, & b\epsilon, & c\epsilon \\ c\epsilon^{\lambda}, & a\epsilon^{\lambda} - x, & b\epsilon^{\lambda} \\ b\epsilon^{\lambda^2}, & c\epsilon^{\lambda^2}, & a\epsilon^{\lambda^2} - x \end{vmatrix} = 0$$

$$\therefore \quad a(\epsilon + \epsilon^{\lambda} + \epsilon^{\lambda^2}) = 1 + \eta + \eta^2 = 0$$

and as $3a = -1$, we must have $\epsilon + \epsilon^{\lambda} + \epsilon^{\lambda^2} = 0$ which cannot be since q has been assumed > 3 and ϵ is a root of the irreducible equation

$$1 + x + x^2 + \cdots + x^{q-1} = 0.$$

If $V^6 = 1$, we must have first $3a = 0$. Hence the array corresponding to V is of the type

$$\begin{Vmatrix} 0, & b, & c \\ c, & 0, & b \\ b, & c, & 0 \end{Vmatrix}.$$

Its square

$$\begin{Vmatrix} 2bc, & c^2, & b^2 \\ b^2, & 2bc, & c^2 \\ c^2, & b^2, & 2bc \end{Vmatrix}$$

must be a matrix whose cube is unity. Hence again $6bc = 0$, and either b or $c = 0$. Assume for example $b = 0$. Expressing the fact that the multipliers of V have -1 for product we have $c^3 = -1$, hence $c = -1$, $\eta^{\frac{1}{2}}$ or $\eta^{-\frac{1}{2}}$. The values $\eta^{\pm\frac{1}{2}}$ are to be set aside for c must be a number of the domain $K(\epsilon)$ and cannot be a root of unity of degree prime to q. As to -1 it must be set aside for then VS would be a birational transformation with multipliers all -1, and $C_{3p'}$ would be hyperelliptic. Our affirmation is therefore proved.

156. Let us now consider the array

$$\begin{Vmatrix} a, & b, & c \\ b, & c, & a \\ c, & a, & b \end{Vmatrix}.$$

Assume first $V^6 = 1$. The sum of the multipliers is zero and their product -1, hence

$$a + b + c = 0, \qquad \begin{vmatrix} a, & b, & c \\ b, & c, & a \\ c, & a, & b \end{vmatrix} = -1$$

which cannot be since the determinant just written has $a + b + c$ for factor.

It remains to consider $V^2 = 1$. We have then $a + b + c = -2 + 1 = -1$. Moreover since the square of our array is the identical substitution we must have

$$bc + ca + ab = 0,$$
$$\therefore \quad a(-1-a) + bc = 0, \qquad a = bc - a^2,$$

and similarly $b = ca - b^2$, $c = ab - c^2$. Finally since VT^{-1} is of order *three*, the roots of

$$\begin{vmatrix} a\epsilon - x, & b\epsilon, & c\epsilon \\ b\epsilon^{\lambda}, & c\epsilon^{\lambda} - x, & a\epsilon^{\lambda} \\ c\epsilon^{\lambda^2}, & a\epsilon^{\lambda^2}, & b\epsilon^{\lambda^2} - x \end{vmatrix} = 0$$

are $1, \eta, \eta^2$. Their sum and the sum of their double products must be zero, hence $a\epsilon + b\epsilon^{\lambda} + c\epsilon^{\lambda^2} = 0$,

$$\epsilon^{(1+\lambda)}(ac - b^2) + \epsilon^{(\lambda+\lambda^2)}(bc - a^2) + \epsilon^{(1+\lambda^2)}(ab - c^2) = 0.$$

By means of the relations above and since $1 + \lambda + \lambda^2 \equiv 0$, mod. q, this last equation reduces to $a\epsilon^{-1} + b\epsilon^{-\lambda} + c\epsilon^{-\lambda^2} = 0$, from which follows

$$\frac{a}{\epsilon^{\lambda-\lambda^2} - \epsilon^{\lambda^2-\lambda}} = \frac{b}{\epsilon^{1-\lambda} - \epsilon^{\lambda-1}} = \frac{c}{\epsilon^{\lambda^2-1} - \epsilon^{1-\lambda^2}}.$$

The denominators are double the imaginary parts of powers of ϵ not divisible by q, hence they are not zero. Substituting in $bc + ca + ab = 0$, we have:

$$\epsilon^{\lambda^2-\lambda} + \epsilon^{\lambda-\lambda^2} - (\epsilon^3 + \epsilon^{-3}) + \epsilon^{\lambda-1} + \epsilon^{1-\lambda} - (\epsilon^{3(1+\lambda)} + \epsilon^{-3(1+\lambda)})$$
$$+ \epsilon^{1-\lambda^2} + \epsilon^{-1+\lambda^2} - (\epsilon^{3(1+\lambda^2)} + \epsilon^{-3(1+\lambda^2)}) = 0.$$

If we compare the first exponent to the others mod. q, and remember the congruence satisfied by λ, we find that it cannot be equal to any of them unless $\lambda = -2$, $-4/5$ or $-1/5$, mod. q, and since $\lambda^3 \equiv 1$, mod. q, it is easily seen that q must divide one of the integers 9, $126 = 2\cdot 3^2\cdot 7$, $189 = 3^3\cdot 7$ and therefore must be 7. For $q > 7$ the equation which ϵ must satisfy is certainly not its irreducible equation since it has less than $q - 1$ terms, or has $q - 1$ terms perhaps for $q = 13$, but with coefficients certainly not all equal.

The only possibility is then $q = 7$, $p' = 1$, $p = 3$, when $C_{3p'}$ is Klein's quartic. The relation just obtained is identically verified and in fact this curve possesses as shown precisely by Klein a binary transformation such as V and its group is the classical G_{168} generated by S, T, and V. For further

details and in particular for the equations of the group the reader is referred to his work (loc. cit.). *This ends the proof of the theorem of No. 148.*

157. The properties of the curves whose discussion is now complete may be summarized thus: *The curves of minimum genus possessing a cyclic group of order q, odd prime, constitute a finite number of birationally distinct families. Their total group is the cyclic group of order q with the exception of:* (*a*) *A hyperelliptic family present, whatever q, and whose group is of order $2q$ cyclic.* (*b*) *A family present only when $q - 1$ is divisible by three whose group is of order $3q$, unless $q = 7$ when it is the classical G_{168}. The indices of the Jacobi variety are given by*

$$1 + h = 2(1 + k) = 2p = q - 1$$

and the variety is pure except in the case (*b*) *when*

$$1 + h = 2(1 + k) = 6p = 3(q - 1),$$

and the variety is impure.

Remark: The variety of rank q corresponding to the group of order q has no congruence of spaces for $q > 7$, or for $q = 7$ and Klein's quartic, as then the product of the multipliers is $+1$ and the Jacobi variety possesses a triple integral of the first kind (No. 127). For $q = 5$ the first variety is ruled as shown by Enriques and Severi. The only doubtful case is then that of the hyperelliptic curve present for $q = 7$.

§ 3. **Curves with four critical points**

158. Let us consider first two hypergeometric integrals

$$\int_g^h (x - a_1)^{b_1}(x - a_2)^{b_2}(x - y)^{b_3}\,dx,$$

$$\int_g^h (x - a_1)^{b_1'}(x - a_2)^{b_2'}(x - y)^{b_3'}\,dx.$$

We assume that they have a meaning whatever the limits g, h, which requires that

$$b_i > -1, \qquad b_i' > -1 \qquad (i = 1, 2, 3),$$
$$b_1 + b_2 + b_3 < -1, \qquad b_1' + b_2' + b_3' < -1.$$

Let us denote by ω_1, ω_1' the two integrals corresponding to $g = a_1$, $h = y$ and by ω_2, ω_2' those corresponding to $g = a_2$, $h = y$. Can there exist a bilinear relation

$$\gamma_{11}\,\omega_1\,\omega_1' + \gamma_{12}\,\omega_1\,\omega_2' + \gamma_{21}\,\omega_2\,\omega_1' + \gamma_{22}\,\omega_2\,\omega_2' = 0,$$

where the (γ)'s are independent of y? To answer the question set first

$z = \omega_1/\omega_2$, $z' = \omega'_1/\omega'_2$. As is well known z satisfies Schwarz's differential equation *

$$\frac{2\dfrac{dz}{dy}\dfrac{d^3z}{dy^3} - 3\left(\dfrac{d^2z}{dy^2}\right)^2}{2\left(\dfrac{dz}{dy}\right)^2} = \frac{1-\lambda}{2(y-a_1)^2} + \frac{1-\mu}{2(y-a_2)^2} + \frac{\lambda+\mu-\nu-1}{2(y-a_1)(y-a_2)},$$

$$\lambda = (b_1+b_3+1)^2, \qquad \mu = (b_1+b_2+1)^2, \qquad \nu = (b_2+b_3+1)^2.$$

If the bilinear relation in question exists, z', a linear fractional function of z, must satisfy the same differential equation, and therefore

$$(b_i + b_k + 1) = \pm (b'_i + b'_k + 1) \qquad (i \neq k;\ i, k = 1, 2, 3).$$

By considering the various combinations of signs we find the following four possible types of relations:

$$(a) \qquad b_i = b'_i \qquad (i = 1, 2, 3),$$
$$(b) \qquad 1 + b_i = -b'_i \qquad (i = 1, 2, 3),$$
$$(c) \qquad 1 + b_i = -b'_j, \qquad 1 + b_j = -b'_i, \qquad -1 + b_k = b'_1 + b'_2 + b'_3,$$

in which case b_i, b_j, b'_i, b'_j are > 0 and b_k, $b'_k < 0$.

$$(d) \qquad b_i = b'_j, \qquad b_j = b'_i, \qquad -b'_k = b_1 + b_2 + b_3 + 2.$$

The case (a) is to be rejected for then z would be a constant, and when any of the three sets of relations (b), (c) and (d) are satisfied the bilinear relation certainly exists as is known from the theory of Schwarz's differential equations. To calculate the coefficients we recall that according to Picard the group of the hypergeometric differential equation satisfied by ω_1, ω_2 possesses the two fundamental substitutions †

$$(\omega_1, \omega_2;\ \eta_1\omega_1, (\eta_1 - \eta_3)\omega_1 + \omega_2);$$
$$(\omega_1, \omega_2, \omega_1 + (\eta_2 - \eta_3^{-1})\omega_2, \eta_2\omega_2);$$
$$\eta_1 = e^{-2\pi i(b_1+b_3)}, \qquad \eta_2 = e^{2\pi i(b_2+b_3)}, \qquad \eta_3 = e^{-2\pi i b_3}.$$

By accenting all quantities we obtain similarly the group corresponding to ω'_1, ω'_2. The bilinear relation whose existence is discussed must be invariant when corresponding substitutions are applied to the (ω)'s and the (ω')'s. This yields six equations of the first degree between the (γ)'s. It is found that they are sufficient to determine their ratios provided we have

$$\frac{(\eta_1 - \eta_3)(\eta_2 - \eta_3^{-1})}{(1-\eta_1)(1-\eta_2)} = \frac{(\eta'_1 - \eta'_3)(\eta'_2 - \eta_3'^{-1})}{(1-\eta'_1)(1-\eta'_2)}.$$

---

* See Picard *Traité d'Analyse*, vol. 3, second edition, p. 333.

† Picard, loc. cit. p. 324.

This is at once verified for (*b*). As for (*c*) or (*d*) we have either

$$\eta_1' = \eta_1, \qquad \eta_2' = \eta_2, \qquad \eta_3' = \eta_1\,\eta_2^{-1}\,\eta_3^{-1},$$

or

$$\eta_1' = \eta_2, \qquad \eta_2' = \eta_1, \qquad \eta_3' = \eta_1\,\eta_2^{-1}\,\eta_3^{-1},$$

and by means of one or the other of these relations the equation of condition is readily verified, as was to be expected.

159. We are now ready to undertake the investigation of the curve C_p with four critical points. One of these being assumed for the present at infinity, the equation of the curve will be

$$y^q = (x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2}(x - a_3)^{\alpha_3}$$

with the (α)'s positive and $< q$, their sum being prime to q. The genus is $p = q - 1$ and C_p depends upon a single modulus—the anharmonic ratio of the critical (x)'s. We shall assume this modulus arbitrary and propose to determine above all the invariants of the Jacobi variety and next the total group of our curves.

To n_j corresponds a number of integrals of the first kind given by

$$r_j = \left[n_j \frac{(\alpha_1 + \alpha_2 + \alpha_3)}{q}\right] - \left[\frac{n_j\,\alpha_1}{q}\right] - \left[\frac{n_j\,\alpha_2}{q}\right] - \left[\frac{n_j\,\alpha_3}{q}\right],$$

and they are of the form

$$\int (x - a_1)^{b_1^j}(x - a_2)^{b_2^j}(x - a_3)^{b_3^j}\,dx,$$

the (β)'s having the same meaning as previously. If $r_j = 1$ we shall take

$$b_i^j = \beta_i^j \frac{-\,n_j\,\alpha_i}{q} \qquad (i = 1, 2, 3),$$

while if $r_j = 2$ there will be another integral which we shall choose so that it differ from the first only in that $b_1^j = \beta_i^j - (1/q)\,n_j\,\alpha_i + 1$. We can of course choose two other analogous integrals by permuting $1, 2, 3$ but they are linear combinations of the two just considered. We recall that the period matrix Ω is composed with the arrays

$$\tau = \|\,\tau_{j1},\, \tau_{j2}\,\|, \qquad \|\,1,\, \epsilon^{n_j},\, \cdots,\, \epsilon^{(q-2)n_j}\,\|, \qquad (j = 1, 2, \cdots, p),$$

where

$$\tau_{j\mu} = \int_{a_\mu}^{a_{\mu+1}} du_j.$$

160. Since Ω is a Riemann matrix there certainly exists an alternate bilinear form

$$\sum_{\mu,\nu}^{1\ 2} \gamma_{\mu\nu}(\epsilon^{n_j},\, \epsilon^{n_k})\,x_\mu\,y_\nu \tag{6}$$

in the sense of Chapter II. The (γ)'s are such that

$$\gamma_{\mu\nu}(x, y) = -\gamma_{\nu\mu}(y, x);$$
$$\gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_k}) = 0 \qquad \text{if} \qquad n_j + n_k \not\equiv 0, \quad \text{mod. } q.$$

The ratios τ_{j1}/τ_{j2} are certainly variable for otherwise our curves would all have the same period matrix and would not depend upon a variable modulus. It follows that the form (6) is unique.

Can there exist forms of any other type? Whether it is alternate or not assume that such a form leads to an actual relation between the periods of u_j and u_k, that is, that the quantities $\gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_k})$ are not all zero. Then one of the sets of relations (*b*), (*c*), (*d*) of No. 158 must be satisfied. (*b*) leads to

$$n_j \alpha_i \equiv -n_h \alpha_i, \quad \text{mod. } q \qquad (i = 1, 2, 3, 4);$$
$$\therefore \quad n_j + n_h \equiv 0, \quad \text{mod. } q,$$

that is, the (γ)'s are all zero except when ϵ^{n_j} and ϵ^{n_k} are conjugate. The calculation of No. 158 shows that the bilinear relation existing must be unique and as in the case considered (6) already is one there can be no other.

The conditions (*c*) lead to, for example,

$$n_j \alpha_1 = -n_h \alpha_2, \qquad n_j \alpha_2 \equiv -n_h \alpha_1, \text{ mod. } q.$$
$$n_j \alpha_3 = -n_h(\alpha_1 + \alpha_2 + \alpha_3) \equiv n_h \alpha_4, \text{ mod. } q.$$

Hence mod. q, either

$$\alpha_1 \equiv \alpha_2, \qquad n_j \equiv -n_h,$$

or

$$\alpha_1 \equiv -\alpha_2, \qquad n_j \equiv n_h, \qquad \alpha_3 \equiv -\alpha_4.$$

In the first case we are in the same situation as before. In the second C_p is birationally equivalent to

$$y^q = \frac{x - a_1}{x - a_2}\left(\frac{x - a_3}{x - a_4}\right)^{\alpha}, \qquad 0 < \alpha < q. \tag{7}$$

We can take $\alpha_1 = 1$, $\alpha_2 = q - 1$, $\alpha_3 = \alpha$, and find that

$$r_j = \left[\frac{n_j(q + \alpha)}{q}\right] - \left[\frac{n_j}{q}\right] - \left[\frac{n_j(q - 1)}{q}\right] - \left[\frac{n_j \alpha}{q}\right] = 1$$

which shows that for each value of n_j there is only one integral and a bilinear relation such as contemplated in the second case cannot exist. The discussion of conditions (*d*) is the same as for (*c*) and the answer negative as well. *Hence Ω possesses no other bilinear form than* (6).

161. To determine h, k we must find out if there are other curves than (7) for which $r_j = 1$ whatever j. We shall see that this is not the case.

If $r_j = 1$ whatever j, Ω is composed with arrays

$$\| \tau_{j1}, \tau_{j2} \|, \qquad \| 1, \epsilon^j, \epsilon^{2j}, \cdots, \epsilon^{(q-2)j} \| \qquad (j = 1, 2, \cdots, q-1 = p).$$

The calculation outlined in No. 158 leads to the relation

$$\tau_{q-j,\,2}\,\tau_{j1} - \epsilon^j\,\tau_{q-j,\,1}\,\tau_{j,\,2} = 0.$$

$$\therefore \quad \frac{\tau_{q-j,\,2}}{\tau_{q-j,\,1}} = \frac{\epsilon^j\,\tau_{j,\,2}}{\tau_{j,\,1}} = \epsilon^j \cdot \tau_j$$

and therefore Ω can be put in the following form, where only the j-th and $(q-j)$-th rows are written:

$$\Omega \equiv \left\| \begin{array}{cccccccc} 1, & \epsilon^j, & \epsilon^{2j}, & \cdots, & \epsilon^{(q-2)j}; & \tau_j, & \epsilon^j\,\tau_j, & \cdots, & \tau_j\,\epsilon^{(q-2)j} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \epsilon^{-j}, & \epsilon^{-2j}, & \cdots, & \epsilon^{-(q-2)j}; & \tau_j\,\epsilon^j, & \tau_j, & \cdots, & \tau_j\,\epsilon^{-(q-3)j} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array} \right\|.$$

Denote respectively by δ_μ, $\overline{\delta_\mu}$, the cycles corresponding to the periods ϵ^μ, $\tau_1\,\epsilon^\mu$, in the first line, the indices being taken mod. q. If we apply to the integrals and the cycles the binary permutations

$$u'_j = u_{q-j} \qquad (j = 1, 2, \cdots, p)$$

$$\delta'_\mu \sim \delta_{-\mu}; \qquad \overline{\delta'_\mu} \sim \delta_{1-\mu} \qquad (\mu = 0, 1, 2, \cdots, q-1)$$

Ω is unchanged. Hence C_p possesses a corresponding binary transformation U whose genus is $\frac{1}{2}p$ for it maintains invariant the integrals $u_j + u_{q-j}$ and no others.

Let (x, y) be any point of C_p, (x', y') its transformed by U. The integrals of the first kind are all of the form

$$\int \frac{\prod^{(i)} (x - a_i)^{\gamma_i}\,dx}{y^n}.$$

By reasoning as in No. 145 we find therefore again that U merely permutes the critical points. The equations of U are of type (2) and it is not the ordinary transformation present in hyperelliptic curves since its genus is not zero. Besides U must permute every critical point for if it maintained two of them fixed, the anharmonic ratio of the (a)'s would not be variable as was assumed. If then U permutes A_1 with A_2 and A_3 with A_4, we must have (No. 138)

$$\frac{\alpha_2}{\alpha_1} \equiv \frac{\alpha_1}{\alpha_2}, \qquad \frac{\alpha_4}{\alpha_3} \equiv \frac{\alpha_3}{\alpha_4}, \qquad \text{mod. } q$$

and as we may always take $\alpha_1 = 1$, it is seen at once that we fall back upon (7), as was to be proved.

In accordance then with Chapter II, *if there are four arbitrary critical points,*

the Jacobi variety is pure, its indices being given by

$$(1 + h) = 2(1 + k) = p = q - 1$$

unless we deal with (7) *when the variety is impure and*

$$1 + h = 2(q - 1) = 2p, \qquad 1 + k = 3(q - 1).$$

162. Let us investigate more closely the question of birational transformations. We know that if C_p is not of type (7) its total group is cyclic of order q (No. 142). It remains to consider the curves (7).

In the first place if $\alpha = 1$, the curve is hyperelliptic. The ordinary transformation then present shall be denoted by S, and the binary transformation of genus p', as before, by U. We propose to show that *in general C_p possesses no other transformations than S, T, U and the products of their powers.*

In the first place the birational transformations T^k, $T^k\, U$, define the two multiplications

$$u_j' = \epsilon^{kj}\, u_j, \qquad u_j' = \epsilon^{kj}\, u_{q-j} \qquad (j = 1, 2, \cdots, p),$$

and among those $2q$ multiplications exactly $2(q - 1) = 1 + h$ are linearly independent. If we write the integrals in suitable order the most general multiplications will be represented by an array

$$\left\| \begin{matrix} B_1, & 0, & \cdots, & 0 \\ 0, & B_2, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots, & B_{\frac{1}{2}p} \end{matrix} \right\| ; \qquad B_j = \left\| \begin{matrix} g(\epsilon^j), & h(\epsilon^j) \\ h(\epsilon^{-j}), & g(\epsilon^{-j}) \end{matrix} \right\|,$$

where g, h are polynomials with rational coefficients. The array B_j may be written more simply

$$\left\| \begin{matrix} g, & h \\ \bar{h}, & \bar{g} \end{matrix} \right\|.$$

We first remark that if C_p is hyperelliptic A_1 may be permuted with the three other (A)'s by one of the three transformations S, U, $SU = US$, while if C_p is not hyperelliptic, A may be permuted with only one of these points, and that by means of U. But as a matter of fact the two cases, hyperelliptic and the other, need not be separated in the discussion.

163. Let us now assume that there exists a transformation V of C_p not a product of powers of those already known. The binary transformation $W = V^{-1}\, U \cdot V$ may or may not permute the (A)'s among themselves. We propose to show that in both cases we are led to an impossibility.

To begin with if W permutes the (A)'s merely among themselves it must belong to one of the three types UT^k, ST^k, UST^k. But if $T^k \neq 1$, these transformations are of order $2q$ at least as seen by a reference to their complex multiplications. Hence necessarily $T^k = 1$, and $UV = VU$, VS or VUS.

If V corresponds to the array of the (B)'s, we obtain by comparison of the arrays for UV with those of the other three substitutions, one of the systems of relations

$$\begin{array}{lll} (a) & g = \bar{g}, & h = \bar{h}, \\ (b) & g = -\bar{h}, & \\ (c) & g = -\bar{g}, & h = -\bar{h}. \end{array}$$

The equation in the multipliers of V is

$$\begin{vmatrix} g - x, & h \\ \bar{h}, & \bar{g} - x \end{vmatrix} = 0.$$

This equation must be reducible in $K(\epsilon)$, whence, as in Nos. 149, 151, the only possible systems of multipliers $(1, -1)$, (η, η^{-1}), $(i, -i)$, $(\eta^{\frac{1}{2}}, \eta^{-\frac{1}{2}})$, $(\epsilon^k, \epsilon^{-k})$, $(-\epsilon^k, -\epsilon^{-k})$, corresponding to the orders $\nu = 2, 3, 4, 6, q, 2q$ for V.

164. In the case of relations (*a*), g and h are real and the equation in the multipliers is $x^2 - 2gx + g^2 - h^2 = 0$. Let x_1, x_2 be its roots. When $x_1 = 1$, $x_2 = -1$, we have $g = 0$, $h = \pm 1$, hence $V = U$ or SU.* In the other cases h takes the values $\pm i$, $\pm \frac{i\sqrt{3}}{2}$, $\pm \frac{(\epsilon^k - \epsilon^{-k})}{2}$, all imaginary whereas h must be real.

In the case of relations (*b*) the equation in the multipliers is

$$x^2 - (g + \bar{g})x = 0$$

and must be rejected since no multipliers can be zero.

Finally in the case of relations (*c*), the equation is $x^2 + h^2 = 0$. Since h is purely imaginary, $h^2 = x_1 x_2$ is a negative real number, and therefore necessarily $x_1 = 1$, $x_2 = -1$, $h = \pm i$. But h is a number of the domain $K(\epsilon)$, and therefore cannot be a root of unity of degree prime to q. Hence V cannot correspond to any relations such as those just discussed.

165. Let us assume now that the binary transformation W of No. 163 permutes the (A)'s with points of another similar set. The multipliers of W must be $1, -1$, since it is not S, and if it corresponds to the array of (B)'s, we must have $g + \bar{g} = 0$. g is therefore purely imaginary. If we set $\epsilon^k + \epsilon^{-k} = \eta_k$, $\epsilon^k - \epsilon^{-k} = \zeta_k$, the (η)'s are real and the (ζ)'s pure imaginary, hence

$$g = \sum_{i=1}^{\frac{q-1}{2}} a_i \zeta_i \qquad (a_i \text{ rational number}).$$

To TW corresponds an array of (B)'s with $g\epsilon$ in place of g. More exactly, to

* For by the remark at the end of No. 141 it is sufficient to show that to $V^{-1}U$ or $V^{-1}SU$ correspond ordinary transformations of the Jacobi variety, and this is readily done.

the B_j of this array corresponds $g(\epsilon^j)\cdot\epsilon^j$, but if ϵ designates a suitably chosen q-th root of unity, any one of these numbers can be set in the form $g\epsilon$. Now if we set $\eta_0 = 2$, it is at once verified that the real part of $\zeta_i\,\epsilon = \frac{1}{2}\zeta_i(\eta_1 + \zeta_1)$ is equal to $\frac{1}{2}\zeta_i\,\zeta_1 = \frac{1}{2}(\eta_{i+1} - \eta_{i-1})$. Hence the double of the real part of $g\epsilon$, or

$$g\epsilon + \bar{g}\epsilon^{-1} = \sum_{i=1}^{\frac{q-1}{2}} a_i(\eta_{i+1} - \eta_{i-1}).$$

Finally since $\eta_j = \eta_{q-j}$, we can write

$$g\epsilon + \bar{g}\epsilon^{-1} = \sum_{i=1}^{\frac{q-1}{2}} a'_i(\eta_{2i} - \eta_{2(i-1)}),$$

where the (a')'s are merely the (a)'s written in different order. If we write the equation in the multipliers of TW we see at once that this expression can only have the values $0, \pm 1, \pm(\epsilon^k + \epsilon^{-k})$.

In the first case the (a')'s and therefore the (a)'s must all be zero. The second leads to

$$a'_1 = \pm\tfrac{1}{2}, \qquad a'_1 = a'_2 = \cdots = a'_{\frac{q-1}{2}},$$

hence $g\epsilon + \bar{g}\epsilon^{-1} = \pm\frac{1}{2}\eta_{\frac{q-1}{2}} \pm 1 \neq \pm 1$, and therefore cannot occur at all. In the third case we have, s being a suitable integer between 0 and $q-1$, $g\epsilon + \bar{g}\epsilon^{-1} = \pm\,\eta_{2s}$;

$$\therefore\quad a'_s - a'_{s+1} = \pm 1, \qquad a'_i = a'_s, \qquad i < s; \qquad a'_{s+i} = a'_{s+1}.$$

Hence then $g\epsilon + \bar{g}\epsilon^{-1} = -2a'_s \pm \eta_{2s} + 2a'_{s+1}\,\eta_{q-1}$ which can only be if $a'_{s+1} = a'_s = 0$ and we have here again a contradiction.

The only possibility is then $g = 0$. But in this case UW corresponds to a multiplication of type $u'_j = \lambda_j\,u_j$, where u_j is the integral which T multiplies by ϵ^j. This multiplication is permutable with T, cyclic, and therefore, by a previous remark, $W = US^i\,T^k$ or UT^k and hence must permute the (A)'s among themselves, contrary to the assumptions made.

This completes the proof of the non existence of any transformations of C_p other than those belonging to the group generated by S, T and U.

166. It is at once verified that $T^k\,U = UT^{-k}$, hence every substitution of the group is of the form $S^i\,U^j\,T^k$ if C_p is hyperelliptic, or $U^j\,T^k$ if it is not. Hence *if C_p is not hyperelliptic, that is, if the integer α in* (7) *is* > 1, *the group is of order* $2q$, *while if the curve is hyperlliptic the order is* $4q$.

Observe that the curve can be reduced to the form

$$y^q = \left(\frac{x-a}{ax-1}\right)\left(\frac{x+a}{ax+1}\right)^{\alpha},$$

the equations of U being then $x' = -x$, $y' = y^{-1}$. For $\alpha = 1$ we have, besides, S, whose equations are $x' = -x$, $y' = y$. The parameter a may be taken as modulus of the curve.

Remark: For particular values of the modulus of which the curves with four critical points depend, there will be other birational transformations different from those considered. For example

$$y^q = (x-1)(x-\eta)(x-\eta^2), \qquad \eta = e^{\frac{2\pi i}{3}},$$

possesses an obvious cyclic transformation of order three.

§ 4. Curves with $r + 2 > 4$ critical points.

167. We shall take the equation in the form

$$y^q = \prod_{i=1}^{r+1}(x-a_i)^{\alpha_i}, \tag{8}$$

the (α)'s of index $< r+2$ and their sum being prime to q, with a_{r+2} at infinity.

We may choose for the r_j integrals of the first kind corresponding to n_j, the set

$$\int \frac{(x-a_1)^{\gamma_j}\prod^{(i)}(x-a_i)^{\overset{j}{\beta_i}}\,dx}{y^{n_j}} \qquad (\gamma_j = 1, 2, \cdots, r_j).$$

Now the sums $\alpha_i + \alpha_j$ cannot all be divisible by q. For then if r is odd, $\sum_{i=1}^{r+1}\alpha_i$ would be divisible by q, while if r is even

$$2\sum \alpha_i = \alpha_1 + \alpha_2 + \sum_{i=2}^{r+1}\alpha_i + (\alpha_1 + \sum_{i=3}^{r+1}\alpha_i)$$

would be also, leading again to the divisibility of the same sum by q.

Let us observe that since $r > 2$ we may arrange matters so that there will be at least three sums $\alpha_\mu + \alpha_{\mu+1}$ not divisible by q. For the worst conditions obtained are when:

(*a*) $r = 3$ and we have a set of five exponents corresponding to the five critical points, such as: $\alpha, -\alpha, \alpha, \alpha', \alpha''$. Then $\alpha + \alpha' + \alpha'' \equiv 0$, mod. q, and neither α' nor α'' are $\equiv -\alpha$. One of them however may be $\equiv \alpha$. In this case the exponents in suitable order form a set such as $\alpha, \alpha, \alpha, \alpha'$, $-\alpha$, and the sums 2α, 2α, $\alpha + \alpha'$ are not divisible by q.

(*b*) $r = 4$ and the set of exponents is $\alpha, -\alpha, \alpha, -\alpha, \alpha - \alpha$. In another order they form the set $\alpha, \alpha, \alpha, -\alpha, -\alpha, -\alpha$, for which the assertion is at once verified.

Let then $\alpha_1 + \alpha_2 \not\equiv 0$, mod. q, and make a_1 tend towards a_2. Some of the integrals of the first kind will preserve their character for the curve $C_{p'}$ limit

of C_p, where $p' = \frac{1}{2}(r-1)(q-1)$. I say that the integrals of the first kind corresponding to n_j for $C_{p'}$ will be linearly dependent upon these. For the limiting integrals which preserve their character form the set

$$\int (x-a_1)^{b_1'} \prod_{i=3}^{r+1}{}' (x-a_i)^{b_i}\, dx,$$

where the (b)'s have the same value as above, and

$$b_1' = \frac{n_j(\alpha_1+\alpha_2)}{q} - \left[\frac{n_j(\alpha_1+\alpha_2)}{q}\right] + \gamma.$$

We must determine the range of the positive integer γ. Recalling that

$$\beta_i^j = \frac{-n_j\,\alpha_i}{q} + \left[\frac{n_j\,\alpha_i}{q}\right] < 0$$

we see that if the integer $[-\beta_1^j - \beta_2^j]$, which < 2, is equal to unity, we must take $\gamma \geqq 1$, while if $[-\beta_1^j - \beta_2^j] = 0$ we must have only $\gamma \geqq 0$. On the other hand the upper limit of γ is r_j' corresponding to r_j for C_p. But $r_j' = r_j - [-\beta_1^j - \beta_2^j]$, and hence in all cases γ takes r_j consecutive values. As the limiting integrals are obviously independent our assertion is proved.

168. I say that if the array τ possesses the bilinear form

$$\sum \gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_k})\, x_\mu\, y_\nu$$

then the coefficients $\gamma_{\mu\nu}$ vanish when ϵ^{n_j}, ϵ^{n_k} are not conjugate, that is when $n_j + n_k \not\equiv 0$, mod. q. Since this has been proved for $r = 2$, we may assume it correct for a curve with less than $r+2$ critical points, then prove it for a curve with that number of critical points.

Assume then first that the theorem is untrue. If the (γ)'s are not zero for a particular pair of exponents n_j, n_k not congruent mod. q, they are not zero for any pair n, cn, where $c \equiv n_k/n_j$, mod. q, and hence if we replace in $\sum \gamma_{\mu\nu}(\epsilon^n, \epsilon^{cn})\, x_\mu\, y_\nu$ the (x)'s by the elements of a row of τ corresponding to ϵ^n and the (y)'s by the elements of a row corresponding to ϵ^{cn}, then the form vanishes identically. Let us assume that there is at least one case where the corresponding integers r_j, r_k are both > 1—for example let this be so for n_j, n_k themselves. The critical points being ranged in proper order there will be three distinct sums $\alpha_\mu + \alpha_{\mu+1}$, $\alpha_{\mu'} + \alpha_{\mu'+1}$, $\alpha_{\mu''} + \alpha_{\mu''+1}$, not divisible by q. If a_μ is made to tend towards $a_{\mu+1}$ there will be two integrals of the first kind corresponding to n_j and n_k preserving their character for the limiting curve $C_{p'}$. Let $\tau_{j\nu}$, $\tau_{k\rho}$ $(\nu, \rho = 1, 2, \cdots, r)$ be the corresponding elements of the array τ. We have then $\sum \gamma_{\nu\rho}(\epsilon^{n_j}, \epsilon^{n_k})\, \tau_{j\nu}\, \tau_{k\rho} = 0$. Passing to the limit, $\tau_{j\nu}$, $\tau_{k\rho}$ become similar periods of the limiting integrals, say

$\tau'_{j\nu}$, $\tau'_{k\rho}$, except that $\tau'_{j\mu} = \tau'_{k\mu} = 0$. Hence then

$$\sum_{\nu,\rho\neq\mu} \gamma_{\nu\rho}(\epsilon^{n_j}, \epsilon^{n_k})\tau'_{j\nu}\tau'_{k\rho} = 0,$$

and there will be such a relation for every pair of integrals of $C_{p'}$ corresponding to n_j, n_k, and even more generally to cn_j, cn_k. According to the assumptions we have therefore

$$\gamma_{\nu\rho}(\epsilon^{n_j}, \epsilon^{n_k}) = 0 \qquad (\nu, \rho \neq \mu.)$$

If we reason similarly when μ is replaced first by μ', then by μ'', we find successively

$$\gamma_{\mu\rho}(\epsilon^{n_j}, \epsilon^{n_k}) = \gamma_{\rho\mu}(\epsilon^{n_j}, \epsilon^{n_k}) = 0, \qquad \rho \neq \mu';$$
$$\gamma_{\mu\mu'}(\epsilon^{n_j}, \epsilon^{n_k}) = \gamma_{\mu'\mu}(\epsilon^{n_j}, \epsilon^{n_k}) = 0,$$

which completes the proof in the case considered.

169. The above may cease to apply: (*a*) When the integers r_j corresponding to the sequence of exponents l, cl, $c^2 l$, $c^3 l$, $\cdots$, are alternately $+1$ and $r - 1$, and the limiting curve $C_{p'}$ possesses no integrals corresponding to the exponents for which $r = 1$. But in this case the numbers r_j corresponding to $C_{p'}$ are all $r - 1$ which is impossible if $r > 2$. The proof can therefore still be applied as between integrals corresponding to two exponents $c^s l$, $c^{s+1} l$, leading to $\gamma_{\mu\nu}(\epsilon^{c^s l}, \epsilon^{c^{s+1} l}) = 0$. But since the (γ)'s are polynomials with rational coefficients, it follows that $\gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{cn_j}) = \gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_k}) = 0$. (*b*) When $n_j = n_k$, $r = 3$. In this case we are not certain that to a bilinear relation between the periods of C_p corresponds after passing to the limit a similar one for $C_{p'}$, at least if all the numbers r_j of this last curve are equal to unity. Generally speaking let τ'_{j1}, τ'_{j2}, τ'_{j3} and τ''_{j1}, τ''_{j2}, τ''_{j3} be two lines of τ corresponding to n_j. By assumption then $\sum \gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_j})\tau'_{j\mu}\tau''_{j\nu} = 0$ with the relations $\gamma_{\mu\nu}(\epsilon, \epsilon) = -\gamma_{\nu\mu}(\epsilon, \epsilon)$, for otherwise there would exist a bilinear relation between the elements of every row of τ, the impossibility of which may be established as in No. 168. We have then in

$$\sum \gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_j})x_\mu y_\nu = 0$$

the equation of a plane "line complex."—We recall that in a space of an even number of dimensions linear complexes are degenerate. Hence there must exist a unique point (τ_1, τ_2, τ_3) of the plane, conjugate of both $(\tau'_1, \tau'_2, \tau'_3)$ and $(\tau''_1, \tau''_2, \tau''_3)$, relatively to the above complex. On the other hand when the moduli of C_p vary these points remain conjugate with respect to the same complex. But when the (a)'s describe closed paths the (τ')'s and (τ'')'s are transformed by a certain discontinuous projective group whose fundamental operations have been given by Picard.* Since the point (τ_1, τ_2, τ_3) is unique it must be maintained invariant by this group. However a glance at

*Annales de l' École Normale (1885).

the equation of its operations show that they leave no point invariant. We have therefore an impossibility, hence $\gamma_{\mu\nu}(\epsilon^{n_j}, \epsilon^{n_\nu}) = 0$.

170. It follows that *for the curves with more than four critical points in general position the period matrix possesses a minimum number of bilinear forms and consequently for the Jacobi variety* $1 + h = 2(1 + k) = q - 1$.

171. CONCLUSION. Our whole discussion may be summarized thus: The curves possessing a cyclic group of order q odd prime, of genus zero, with arbitrary coincidence points, do not possess in general any other birational transformations and their Jacobi varieties are pure with

$$1 + h = 2(1 + k) = q - 1.$$

Exception must be made for the curves birationally equivalent to the following:

(I) $$y^q = x^2 - a^2.$$

The group is then of order $2q$, cyclic, the rest being as in the general case.

(II) $$y^q = (x - 1)(x - \eta)^\lambda (x - \eta^2)^{\lambda^2}$$
$$\left(\frac{q-1}{3}\text{ integer;} \qquad \eta = e^{\frac{2\pi i}{3}}; \qquad \lambda^3 \equiv 1 \text{ mod. } q\right).$$

The group is of order $3q$ if $q > 7$, of order 168 if $q = 7$ (curve reducible to Klein's quartic). The Jacobi variety is impure with

$$1 + h = 2(1 + k) = 6p = 3(q - 1).$$

(III) $$y^q = \frac{(x - a)}{(ax - 1)}\left(\frac{x + a}{ax + 1}\right)^\alpha.$$

The order of the group is $2q$ if $\alpha^2 \not\equiv 1$, mod. q, $4q$ in the opposite case. The Jacobi variety is impure with

$$1 + h = 2(q - 1), \qquad 1 + k = 3/2(q - 1).$$

UNIVERSITY OF KANSAS,
LAWRENCE, KANSAS.